数学名著译丛

代数学

I

B. L. 范德瓦尔登

科学出版社

数学名著譯丛

代 数 学

I

B. L. 范德瓦尔登 著

丁石孙 曾肯成 郝鈵新 譯

万哲先 校

科 学 出 版 社

1963

B. L. VAN DER WAERDEN

ALGEBRA

I

SPRINGER-VERLAG

1955 VIERTE AUFLAGE

内容简介

全书共分两卷，涉及的面很广，可説概括了1920—1940年左右代数学的主要成就，也包括了1940年以后代数学的新进展，是代数学的經典著作之一。本书是第一卷，分十章：前三章以最小的篇幅包括了为所有其余各章作准备的知識，即有关(1)集合，(2)羣，(3)环、理想和域的最基本的概念；其余各章主要講述交換域的理論。

数学名著譯丛

代　数　学

I

B. L. 范德瓦尔登 著

丁石孙　曾肯成　郝鈵新 譯

万哲先校

*

科学出版社出版（北京朝阳門大街117号）
北京市书刊出版业營业許可証出字第061号

中国科学院印刷厂印刷　新华书店总經售

*

1963年7月第一版　书号：2753
1963年7月第一次印刷　字数：272,000
(京) 精：1—2,700　开本：850×1168 1/32
平：1—3,500　印张：12　插頁：3

定价：精装本 2.50 元
平装本 2.00 元

中譯本序言

代数学是数学的一个重要的基础的分支，历史悠久．我国古代在代数学方面，有光辉的成就．一百多年来，尤其是本世紀以来，随着数学的发展以及应用的需要，代数学的研究对象以及研究方法发生了巨大的变革．一系列的新的代数領域被建立起来，大大地扩充了代数学的研究范围，形成了所謂近世代数学．它与以代数方程的根的計算与分布为研究中心的古典代数学有所不同，它是以研究数字、文字和更一般元素的代数运算的規律及各种代数結构——羣、环、代数、域、格等——的性质为其中心問題的．由于代数运算貫串在任何数学理論和应用問題里，也由于代数結构及其中元素的一般性，近世代数学的研究在数学中是具有基本性的．它的方法和結果滲透到那些与它相接近的各个不同的数学分支中，成为一些有着新面貌和新內容的数学領域——代数数論、代数几何、拓扑代数、Lie 羣和 Lie 代数、代数拓扑、泛函分析等．这样，近世代数学就对于全部现代数学的发展有着显著的影响，并且对于一些其它的科学領域（如理論物理学、計算机原理等）也有較直接的应用．

历史上，近世代数学可以說是从 19 世紀之初发生的，Galois 应用羣的概念对于高次代数方程是否可以用根式来解的問題进行了研究并給出彻底的解答，他可以說是近世代数学的創始者．从那时起，近世代数学由萌芽而成长而发达．大概由 19 世紀的末叶开始，羣以及紧相联系着的不变量的概念，在几何上、在分析上以

及在理論物理上，都发生了重大的影响。深刻研究羣以及其它相关的概念，如环、理想、綫性空間、代数等，应用于代数学各个部分，这就形成近世代数学更进一步的演进，完成了以前独立发展着的三个主要方面——代数数論、綫性代数及代数、羣論——的綜合。对这一步統一的工作，近代德国代数学派起了主要的作用。由 Dedekind 及 Hilbert 于上世紀末叶的工作开始，Steinitz 于1911 年发表的論文对于代数学抽象化工作貢献很大，其后自 1920 年左右起以 Noether 和 Artin 及她和他的学生們为中心，近世代数学的发展极为灿烂。

Van der Waerden 根据 Noether 和 Artin 的講稿写成“近世代数学”(Moderne Algebra)，綜合近世代数学各方面工作于一书。书分上下两册，第一版于 1930—1931 年分别出版。自出版后，这本书对于近世代数学的传播和发展起了巨大的推动作用。到1959—1960 年，上下两册已分别出到第五版和第四版。时至今日，这本书仍然是在近世代数学方面进行学习和开展科学研究的一部好书。

当然，近世代数学是不断向前发展的。本世紀三十年代当时所謂近世代数学的一些基本內容已經逐渐成为每个近代数学工作者必备的理論知識，所以本书由五十年代第四版起就去掉“近世”两字而改名为“代数学”，同时做了較大的增补和改写，但仍保持着原来的基本内容和风格。至于 Jacobson 的“抽象代数学講义”和 Bourbaki 的“代数学”等书，則出版較后而风格和內容亦有异。

本书的第二版曾有武汉大学故教授萧君絳先生譯本，流传不广，文字亦較艰澀。华罗庚先生于 1938—1939 年在昆明西南联合大学講授近世代数課程时，曾以本书上册为参考編写講义，变动較

大而非全文照譯。 1961 年 9 月国内代数学工作者于北京頤和园举行座談会时，皆認为此书新版有迅速譯出之必要。經过一年，由曹錫华、方抒先、丁石孙、曾肯成、郝鋼新諸同志集体合作譯出第一、二卷。 今后当能对代数学的教学及科学研究起較大的推动作用。更希望国内代数学工作者在教学和科学研究实践中有自著的书籍写成出版。

段 学 复

1962 年 10 月 11 日序于
北京大学数学力学系

第三版前言的一部分

在第二版中，我已經严格地建立了賦值論．賦值論在数論与代数几何中日益表現了它的重要性，因之我把賦值論的一章写得更加詳細与清楚了．

根据許多人的要求，我把在第二版去掉了的关于良序与超限归納的两节又加了进来，在这个基础之上，又把 Steinitz 的域論以最一般的形式写了出来．

按照 Zariski 的意見，多項式概念的引入变得容易理解了．范数与迹的理論也有改进之必要，这是 Peremans 先生向我友好地指出的．

B. L. 范德瓦尔登

Laren (Nordholland)，1950 年 7 月

第四版前言

最近完全出乎意外去世的代数学家与数論专家 Brandt 在德国数学会的协会年报 55 卷中对本书第三版写了如下的評論："关于书名，如果在第四版能够改为更簡单的，但是更确切的书名'代数学'，我将感到很高兴．象这样一部过去、现在以及将来都是最好的数学书，书名不应該引起人們如此的疑惑，似乎它是追随一种时髦的式样，它在昨天还不被人們知道，可是明天可能将被忘掉．"

根据这个意見，我把书名改成了"代数学"．

按照 M. Deuring 的建議，"超复数"概念的定义改得更为合适，同时分圓域的 Galois 理論在它对于循环域理論的应用中显得更加完整。

基于各地来信，还作了許多小的修改，我在这里对所有来信的人表示感謝。

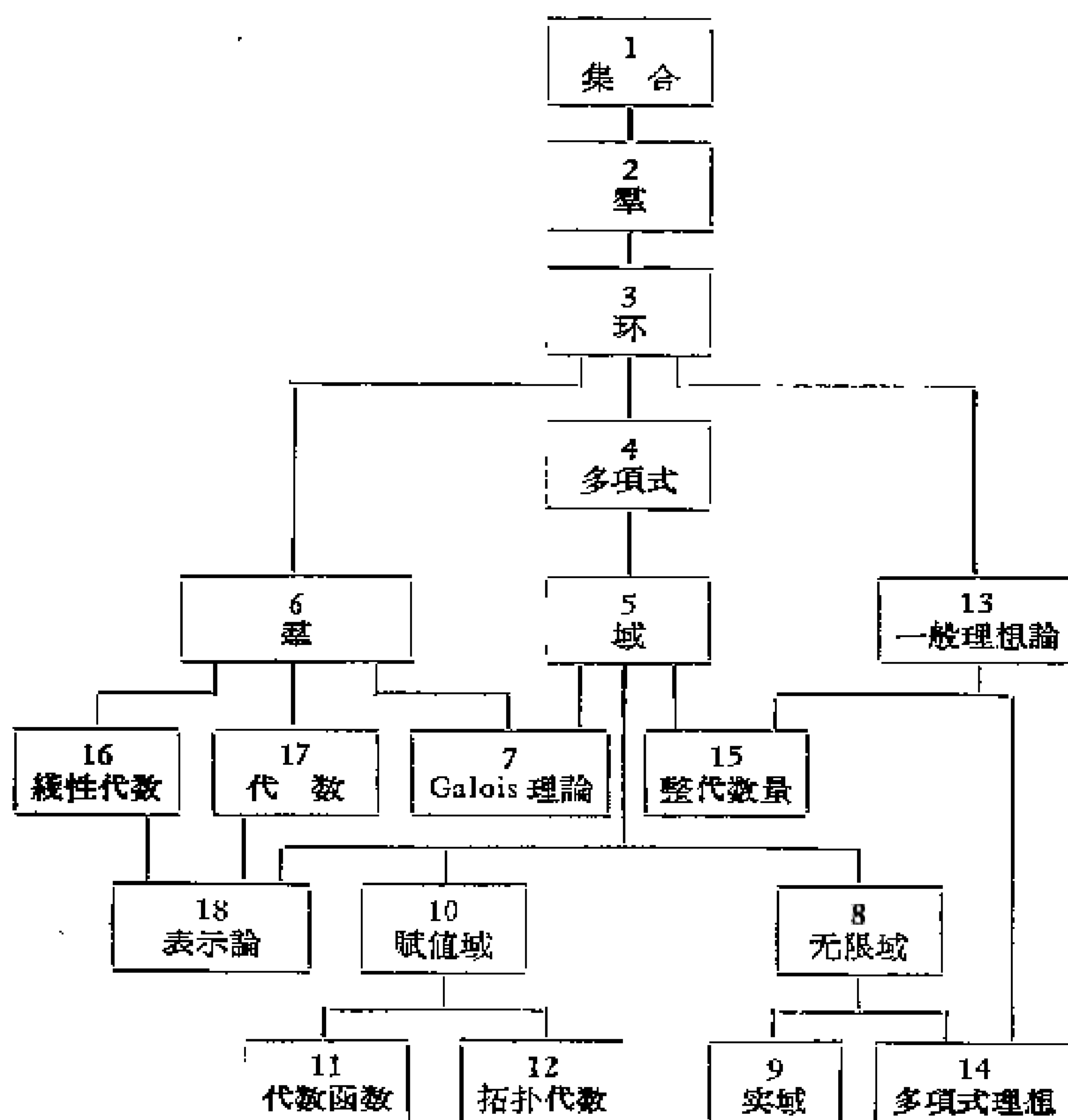
B. L. 范德瓦尔登

Zürich 1955 年 3 月

目　　录

全书綜覽图

I，II 两卷中各章总覽及其邏輯关系



引　　言

本书的目的　"抽象的"、"形式的"或"公理化的"方向在代数学的領域中造成了新的高涨，特别在羣論、域論、賦值論、理想論和超复系理論等部門中引起了一系列新概念的形成，建立了許多新的联系，并导致了一系列深远的結果。本书的主要目的就是要将讀者引入整个这一概念世界。

以这样一些一般的概念和方法作为前导，古典代数学中的个别結果也将要在近世代数的范围之內获得适当的地位。

材料的分配．对讀者的指示　为了充分明晰地展示統治着抽象代数的許多普遍观点，有必要在开头将羣論和初等代数中的基本知識重新作一敘述。

由于最近一个时期出現了羣論、古典代数和域論方面的許多出色的表述，現在已有可能将这些导引性的部分紧凑地(但是完整地)写出来[1]。

另外一个指导原则，就是希望尽可能地作到使每个个别的部

1) 羣論方面参看：

Speiser, A.: Die Theorie der Gruppen von endlicher Ordnung, 2. Aufl. Berlin, Springer, 1927.

域論方面：

Hasse, H.: Höhere Algebra I, II 及 Aufgabensammlung zur Höheren Algebra, Sammlung Göschen, 1926/27.

Haupt, O.: Einführung in die Algebra I, II, Leipzig, 1929.

古典代数方面：

Perron, O.: Algebra I, II, 1927.

綫性代数方面：

Dickson, L. E.: Modern algebraic Theories, Chicago, 1926.

分都能独立地讀懂．只希望了解一般理想論或超复数理論的讀者，就沒有必要去讀 Galois 理論，反之亦然；想要參考消去法或綫性代数的讀者，就可以不必被許多复杂的理想論的概念所吓倒．

材料的分配是这样来安排的：最初三章以最小的篇幅包括了为所有其余各章作准备的知識，即有关 1. 集合；2. 羣；3. 环、理想和域的最基本的概念．第一卷中其余各章主要从事于講述交换域的理論，且主要以 Steinitz 在 *Crelles Journal*, **137** (1910) 发表的奠基性著作为基础．第二卷在尽可能地作到彼此不相依賴的各章中討論了模、环和理想的理論，以及对代数函数、初等因子、超复数和羣表示的应用．

Abel 积分和連續羣的理論不得不从本书中略去，因为对此二者作适当的討論都有必要用到一些超越的概念和方法．其次，由于內容庞大之故，不变量理論也被略去．行列式假定是已知的，幷且只用到很少几次．

为了对本书內容作更进一步的了解，可以查看目录，特别是前面所附的那个綜覽图．从这个图中可以清楚地看到，每一章要利用到前面多少章书．

分插在全书中的許多习題是这样选择的，就是要使讀者能够通过它們来检驗自己是否懂得正文的內容．它們之中也包括了一些在后面有时要用到的例子和补充．解这些习題不需要特别的技巧，要用到的在方括号內也作了提示．

取材来源　这本书部分地是由几次講演发展而成的，这就是：

E. Artin 的代数学講演(汉堡，1926 年夏季)．

E. Artin, W. Blaschke, O. Schreier 和作者所主持的理想論討論班(汉堡，1926/27 冬季)．

E. Noether 关于羣論和超复数理論的两次演講(哥庭根，1924/

25冬季，1926/27 冬季)[1].

本书中的一些新的証明或証明的新的安排，大部分都来自这些演讲和討論班，即使沒有明确指出其来源者也是如此.

1) E. Noether 的后一演讲的整理稿发表在 *Math. Zeitschrift,* **30** (1929), 641—692.

第一章 数与集合

因为在这本书里要用到某些邏輯的和一般数学的概念，对于这些概念初学数学的人很可能还不熟悉，所以在前面我們用較短的一章来介紹一下．在这里我們不打算接触数学基础中的困难問題[1]：我們一直采取“朴素的观点”，当然，我們避免引起詩論的循环定义．有經驗的讀者在这一章只要了解一下符号 $\in$，$\subset$，$\supset$，$\cap$，$\cup$ 与 $\{\cdot\cdot\}$ 的意义，可以略去其余的部分．

§1. 集　　合

作为所有数学討論的起点，我們总是考虑某些确定的对象，譬如数字，字母或者它們的組合． 每个单个元素具有或者不具有的性质就定义一个集合或者类；这个集合的元素就是全体具有这个性质的对象．記号

$$a \in \mathfrak{M}$$

表示：a 是 $\mathfrak{M}$ 的元素． 我們也几何形象地說：a 在 $\mathfrak{M}$ 中． 一个集合称为空的，如果它不包含任何元素．

我們也可以把数(或者字母等)的序列和集合看作对象和集合(我們有时称为第二层集合)的元素．第二层集合又可以是更高层集合的元素，等等．但是在概念形成中，如“所有集合的集合”这类

1) 对于这些問題参看 A. Fraenkel, Einfuhrung in die Mengenlehre (集合論引論), 3. Aufl. (Berlin 1928), 以及 Hilbert-Bernays, Grundlagen der Mathematik (数学基础), Berlin I (1934), II (1939) 和在那里所引的文献．

概念是不允許的，因为它們是造成矛盾的原因；我們常常只从一类預先規定的对象中来造新的集合（新的集合本身不属于这一类对象）。

如果集合 $\mathfrak{N}$ 的全部元素同时是 $\mathfrak{M}$ 的元素，那么 $\mathfrak{N}$ 就称为 $\mathfrak{M}$ 的子集合，記为

$$\mathfrak{N} \subseteq \mathfrak{M}.$$

这时，$\mathfrak{M}$ 也称为 $\mathfrak{N}$ 的包集合，記为

$$\mathfrak{M} \supseteq \mathfrak{N}.$$

由 $\mathfrak{A} \subseteq \mathfrak{B}$ 和 $\mathfrak{B} \subseteq \mathfrak{C}$ 推出 $\mathfrak{A} \subseteq \mathfrak{C}$.

空集合包含在每个集合之中。

如果 $\mathfrak{M}$ 的所有元素全在 $\mathfrak{N}$ 中，同时 $\mathfrak{N}$ 的所有元素全在 $\mathfrak{M}$ 中，那么集合 $\mathfrak{M}$, $\mathfrak{N}$ 称为相等：

$$\mathfrak{M} = \mathfrak{N}.$$

因之，集合相等就表示关系

$$\mathfrak{M} \subseteq \mathfrak{N}, \quad \mathfrak{N} \subseteq \mathfrak{M}$$

同时成立。或者：如果两个集合包含相同的元素，它們就相等。

如果 $\mathfrak{N} \subseteq \mathfrak{M}$，但不 $= \mathfrak{M}$，那么 $\mathfrak{N}$ 就称为 $\mathfrak{M}$ 的眞子集合，$\mathfrak{M}$ 是 $\mathfrak{N}$ 的眞包集合，記为

$$\mathfrak{N} \subset \mathfrak{M}, \quad \mathfrak{M} \supset \mathfrak{N}.$$

因此 $\mathfrak{N} \subset \mathfrak{M}$ 表示，$\mathfrak{N}$ 的元素全在 $\mathfrak{M}$ 中，而在 $\mathfrak{M}$ 中至少有一个元素不在 $\mathfrak{N}$ 中。

設 $\mathfrak{A}$ 与 $\mathfrak{B}$ 是任意的集合。由所有旣属于 $\mathfrak{A}$ 又属于 $\mathfrak{B}$ 的元素組成的集合 $\mathfrak{D}$ 称为集合 $\mathfrak{A}$ 与 $\mathfrak{B}$ 的交，写为

$$\mathfrak{D} = [\mathfrak{A}, \mathfrak{B}] = \mathfrak{A} \cap \mathfrak{B}.$$

$\mathfrak{D}$ 旣是 $\mathfrak{A}$ 的又是 $\mathfrak{B}$ 的子集合，并且每个具有这个性质的集合都包含在 $\mathfrak{D}$ 中。

由属于 $\mathfrak{A}$, $\mathfrak{B}$ 二者之一的全部元素組成的集合 $\mathfrak{V}$ 称为 $\mathfrak{A}$ 与 $\mathfrak{B}$ 的**并**:

$$\mathfrak{V} = \mathfrak{A} \vee \mathfrak{B}.$$

$\mathfrak{V}$ 既包含 $\mathfrak{A}$ 又包含 $\mathfrak{B}$,并且每个同时包含 $\mathfrak{A}$ 与 $\mathfrak{B}$ 的集合一定包含 $\mathfrak{V}$.

同样地,我們定义任意一个集合 $\mathfrak{A}$, $\mathfrak{B}$, $\cdots$ 的集合 Σ 的交与并.对于交(即包含在集合 Σ 的每个集合 $\mathfrak{A}$, $\mathfrak{B}$, $\cdots$ 中的所有元素的集合)記为

$$\mathfrak{D}(\Sigma) = [\mathfrak{A}, \mathfrak{B}, \cdots].$$

如果两个集合的交是空集合,它們就称为**不相交的**,換句話說,它們沒有公共的元素.

如果一个集合是通过元素的列举所給出的,譬如說:集合 $\mathfrak{M}$ 是由元素 a, b, c 組成,那么就写成

$$\mathfrak{M} = \{a, b, c\}.$$

这个写法是合理的,因为按集合相等的定义,一个集合被它全部的元素决定,上面这个集合 $\mathfrak{M}$ 的定义性质就是:与 a 或者 b 或者 c 相等.

§2. 映 射. 势

如果按照某一个規則集合 $\mathfrak{M}$ 的每一个元素 a 都对应于一个新的对象 $\varphi(a)$,那么这个对应就称为一个**函数**,而集合 $\mathfrak{M}$ 称为这个函数的**定义区域**. 如果新的对象 $\varphi(a)$ 全属于一个集合 $\mathfrak{N}$,那么对应 $a \to \varphi(a)$ 也称为**由** $\mathfrak{M}$ **到** $\mathfrak{N}$ **内的映射**. 如果集合 $\mathfrak{N}$ 中每个元素都至少用到一次,那么就称为**由** $\mathfrak{M}$ **到** $\mathfrak{N}$ **上的映射**,而 $\mathfrak{N}$ 称为函数 φ 的**象集合**或者**值区域**,元素 $\varphi(a)$ 称为 a 的**象**,a 称为 $\varphi(a)$ 的**原象**. 象 $\varphi(a)$ 是由 a 唯一决定的,但是反过来 a 并不一

定由 $\varphi(a)$ 唯一决定．在整本书中我們总是用映射这个詞来表示单值映射．

如果 $\mathfrak{N}$ 的每个元素作为象元素恰恰只出现一次，那么这个映射就称为可逆单值的或者 1-1 的．这样就有一个"逆"映射，$\mathfrak{N}$ 中每个元素 b 对应于 $\mathfrak{M}$ 中那个以 b 为象的元素．

两个能够互相 1-1 地映射的集合称为等势的，記为

$$\mathfrak{M} \sim \mathfrak{N}.$$

对于等势的集合我們也説，它們有"相同的势"．

例． 如果我們让每个数 n 对应于数 $2n$，我們就有一个由全体自然数的集合到全体偶数的集合上的 1-1 映射．因之自然数的集合与全体偶数的集合是等势的．

习题． 証明記号 $\sim$ 的以下三个性质：

1．$\mathfrak{A} \sim \mathfrak{A}$．

2．由 $\mathfrak{A} \sim \mathfrak{B}$ 推出 $\mathfrak{B} \sim \mathfrak{A}$．

3．由 $\mathfrak{A} \sim \mathfrak{B}$ 与 $\mathfrak{B} \sim \mathfrak{C}$ 推出 $\mathfrak{A} \sim \mathfrak{C}$．

上面的例子説明，一个集合完全可能与它的一个真子集合是等势的．但是我們在第四节将看到，对于"有限"集合这个情形不可能发生．

§ 3. 自然数序列

我們假定自然数的集合

$$1, 2, 3, \cdots$$

以及这个集合以下的基本性质（Peano 公理）是熟知的：

I. 1 是一个自然数．

II. 在自然数集合中每个数[1] a 有一个确定的后継 a^+．

1）在这里"数"总是指"自然数"．

III. $$a^+ \neq 1,$$
这就是說,沒有数以 1 作为后継.

IV. 由 $a^+ = b^+$ 推出 $a = b$,

这就是說,对于每一个数,沒有或者恰有一个数以它作为后継.

V. "完全归納原理":如果自然数的一个集合包含数 1,并且对于每个属于它的数 a 都包含 a 的后継 a^+, 它就包含全体自然数.

完全归納法这种証明方法就依賴于性质 V. 当我們要証明所有的数都具有一个性質 E 时, 我們就首先对数 1 作証明, 然后在"归納假設"之下, 即假定数 n 具有性質 E, 来証明数 n^+ 具有性質 E. 根据 V,具有性質 E 的自然数的集合必然包含所有的自然数.

两个数的和. 恰有一种方法使每个数偶 x, y 对应于一个自然数,記为 $x + y$, 适合以下关系

(1) $$x + 1 = x^+ \quad \text{对每个 } x,$$

(2) $$x + y^+ = (x + y)^+ \quad \text{对每个 } x \text{ 与每个 } y^{1)}.$$

根据这个定义,我們以后可以把 a^+ 写成 $a + 1$. 它适合运算規律:

(3) $$(a + b) + c = a + (b + c) \quad (\text{"加法的結合律"}).$$

(4) $$a + b = b + a \quad (\text{"加法的交换律"}).$$

(5) 由 $a + b = a + c$ 推出 $b = c$.

两个数的积. 恰有一种方法使每个数偶 x, y 都对应于一个自然数,記为 $x \cdot y$ 或者 xy, 适合以下关系

(6) $$x \cdot 1 = x,$$

(7) $$x \cdot y^+ = x \cdot y + x \quad \text{对每个 } x \text{ 与每个 } y.$$

它适合运算規律:

---

1) 对于这个証明以及本节以下各个定理的証明, 讀者可以参看 E. Landau 的小书: Grundlagen der Analysis (分析基础), Kap. I, Leipzig, 1930 (有中譯本).

(8) $ab\cdot c = a\cdot bc$ （“乘法的結合律”）.

(9) $a\cdot b = b\cdot a$ （“乘法的交換律”）.

(10) $a\cdot(b+c) = a\cdot b + a\cdot c$ （“分配律”）.

(11) 由 $ab = ac$ 推出 $b = c$.

大于与小于. 如果 $a = b + u$，就写成 $a > b$ 或者 $b < a$. 我們可以証明：

对于任意两个数 a，b，以下关系有一个且仅有一个成立

(12) $a < b$， $a = b$， $a > b$.

(13) 由 $a < b$ 与 $b < c$ 推出 $a < c$.

(14) 由 $a < b$ 推出 $a + c < b + c$.

(15) 由 $a < b$ 推出 $ac < bc$.

当 $a > b$ 时，方程 $a = b + u$ 的解 u [根据(5)，是唯一的] 用 $a - b$ 表示. 对于“$a < b$ 或者 $a = b$”我們簡单写为 $a \leqslant b$. 同样地可以定义 $a \geqslant b$.

进一步我們有重要的定理：

自然数的每一个非空集合都有一个最小数，这就是說，有一个小于这个集合中所有其余的数的数.

第二完全归納法就依賴于这条定理. 为了証明所有的数具有性質 E，只要在“归納假設”——即每个 $< n$ 的数已具有性質 E——之下来証任意的数 n 具有性質 E. （特别地，$n = 1$ 要具有这个性質，因为沒有 <1 的数，所以在这个情形“归納假設”沒有[1]）.

---

1) 在根本不存在 A 的情形，我們总是認为断語“所有的 A 都有性質 E”是眞的。同样地，在沒有 x 具有性質 E 的情形，对于任意的性質 F，断語“由 E 推出 F”也被認为是眞的. 这一点与以上所說的，空集合包含在每个集合之中是完全吻合的.

虽然在日常語言中这种用法是不习惯的，但是它的合理性可以由以下这一点得到說明，即只是在这个意义下，断語“由 E 推出 F”才能够无条件地改述为“由非 F 推出非 E”. “由 E（一定）推出 F”的否定語是：存在一个 x，对于它 E 是对的，但 F 是不对的.

归納証明当然必須包括 $n=1$ 的情形，否則是不够的.）于是所有的数必然全具有性质 E. 否則的話，不具有性质 E 的数所成的集合非空. 假如它的最小数为 n，它不具有性质 E，但是所有 $<n$ 的数全具有性质 E，这是不可能的.

与完全归納法的两种形式平行的还有所謂"归納定义(或者构造法)". 如果我們要使每个自然数 x 都与一个新的对象 $\varphi(x)$ 相对应，我們就給出一組"递归的定义关系"，它把函数值 $\varphi(n)$ 与以前的函数值 $\varphi(m)$ $(m<n)$ 联系起来. 对于这組关系我們假定，一旦 $\varphi(m)(m<n)$ 全給出，函数值 $\varphi(n)$ 通过这組关系就唯一地被决定，并且它們同时适合这組关系[1]. 最簡单的一种情形是，对于 $m=n^+$，函数值 $\varphi(n^+)$ 通过 $\varphi(n)$ 表示出来，而对于 $m=1$，函数值 $\varphi(1)$ 被直接給出. 关系(1)，(2)以及(6)，(7)就是例子，通过它們，我們定义了和与积. 現在我們断言：在所作的假定之下，有一个且只有一个函数 $\varphi(n)$，它的值适合所給的关系.

証明. 所謂自然数序列的一个截段 $(1,n)$ 是指 $\leqslant n$ 的数的全体. 我們首先証明：在每一截段 $(1,n)$ 上都恰有一个函数 $\varphi_n(x)$，它定义在这个截段的每个数 x 上并且适合所給的关系. 这个断語对于截段 $(1,1)$ 是对的，并且只要对于截段 $(1,n)$ 成立，对于截段 $(1,n^+)$ 也成立. 因为递归关系給出了函数值 $\varphi(1)$ 并且由前面的函数值 $\varphi(m)=\varphi_n(m)(m\leqslant n)$ 就唯一地决定函数值 $\varphi(n^+)$. 于是我們有了函数 $\varphi_n(x)$ 的序列. 每个函数 $\varphi_n(x)$ 定义在截段 $(1,n)$ 上，同时也定义在較小的截段 $(1,m)$ 上；在那里它也适合定义关系并且与函数 $\varphi_m(x)$ 重合. 因此任意两个函数 $\varphi_n(x)$，$\varphi_m(x)$ 对于它們共同定义的数 x 有相同的函数值.

---

1) 这个假定包括，通过这組关系本身函数值 $\varphi(1)$ 就被决定了，因为在 1 的前面不再有数.

所求的函数 $\varphi(x)$ 必須在**所有的**截段 $(1, n)$ 上都定义并且适合定义关系，因此与函数 $\varphi_n(x)$ 重合． 这样的函数有一个且只有一个：它的值 $\varphi(x)$ 就是所有 $\varphi_n(x)$ 的共同的值．定理得証．

我們將經常用到这种"归納构造法"．

习题． 1．性質 E 对于 $n=3$ 成立，并且如果它对于 $n \geqslant 3$ 成立，那么对于 $n+1$ 也成立．証明：E 对于所有的 $n \geqslant 3$ 的数全成立．

通过符号 $-a$（負整数）与 0（零）的引入我們可以把自然数序列扩充成整数的集合．为了在整数范围内比較清楚地給出記号 $+$，$\cdot$，$<$ 的定义，用自然数偶 (a, b) 来表示整数是方便的，表示如下：

用 $(a+b, b)$ 表示自然数 a，

用 (b, b) 表示 0，

用 $(b, a+b)$ 表示負数 $-a$，

这里 b 是任意的自然数．

每个数都有許多符号 (a, b) 表示；但是每个符号 (a, b) 定义一个且只定义一个整数，即：

当 $a>b$ 表示自然数 $a-b$，

当 $a=b$ 表示数 0，

当 $a<b$ 表示負数 $-(b-a)$．

我們現在定义：

$$(a, b)+(c, d)=(a+c, b+d),$$

$$(a, b) \cdot (c, d)=(ac+bd, ad+bc),$$

$$(a, b)<(c, d) \text{ 或者 } (c, d)>(a, b),$$

$$\text{当} \quad a+d<b+c,$$

不难証明：第一，这些定义与左端符号的选择无关，只要它們所表示的数相同；第二，它們适合运算規律 (3)，(4)，(5)，(8)，(9)，

(10), (12), (13), (14) 以及 (15) 当 $c > 0$; 第三,在扩充了的范围内, 方程 $a + x = b$ 总有唯一解 (解还用 $b - a$ 表示); 第四, $ab = 0$ 当且仅当 $a = 0$ 或者 $b = 0$[1].

习题. 2. 作出以上的証明.

3. 把习题 1 中的 3 换成 0, 作同样的証明.

在整数的初等性质中这里只講了一些以后起作用較大的. 分数的定义与整数的可除性的性質在第三章中講.

§ 4. 有限与可数集合

一个与自然数序列的某一截段 (也就是与 $\leqslant n$ 的自然数的集合)等势的集合称为有限的(或有穷的). 空集合也称为有限的[2].

簡单一些說: 一个集合称为有限的, 如果它的元素可以用 1 到 n 的数目加以編号, 不同的元素有不同的編号, 并且每个 1 到 n 的数目都用到. 因之, 一个有限集合 $\mathfrak{A}$ 的元素可以用 $a_1, \cdots, a_n$ 来代表:

$$\mathfrak{A} = \{a_1, \cdots, a_n\}.$$

习题. 1. 对 n 作完全归納法, 証明, 有限集合 $\mathfrak{A} = \{a_1, \cdots, a_n\}$ 的子集合也是有限的.

不是有限的集合称为无限的(或无穷的). 例如全体整数的集合是无穷的, 这一点下面就要証明.

关于有限集合的基本定理是: 有限集合不能与它的眞包集合等势.

証明. 假定有一个由有限集合 $\mathfrak{A}$ 到它的一个眞包集合 $\mathfrak{B}$ 上

1) 負数与零的另外一个引入的办法可参看 E. Landau: Grundlagen der Analysis, Kap. 4.

2) 对于有限集合的概念的其它定义可参看 A. Tarski: Sur les ensembles finis (关于有限集合), *Fund Math.*, 6 (1925).

的映射．集合 $\mathfrak{A}$ 的元素为 $a_1, \cdots, a_n$．象元素为 $\varphi(a_1), \cdots, \varphi(a_n)$；在它們之中除去出现元素 $a_1, \cdots, a_n$ 外至少还有另外一个元素，我們称之为 a_{n+1}。

对于 $n=1$ 这显然是不可能的．元素 a_1 不可能有两个不相同的象元素 a_1, a_2。

假設对于 $n-1$ 的情形不可能有具有以上性质的映射 φ 已經証明；現在来証 n 的情形．

我們无妨假定 $\varphi(a_n)=a_{n+1}$；假如不是这样，譬如說

$$\varphi(a_n)=a' \qquad (a' \neq a_{n+1})$$

而 a_{n+1} 有另一个原象 a_i：

$$\varphi(a_i)=a_{n+1},$$

于是可以作另一个映射来代替 φ，这个映射使 a_n 对应于 a_{n+1}，a_i 对应于 a'，其余的与 φ 相同．

在函数 φ 之下，子集合 $\mathfrak{A}'=\{a_1, \cdots, a_{n-1}\}$ 映到集合 $\varphi(\mathfrak{A}')$，它就是由 $\varphi(\mathfrak{A})=\mathfrak{Q}$ 中除去元素 $\varphi(a_n)=a_{n+1}$ 所得的集合．

$\varphi(\mathfrak{A}')$ 包含元素 $a_1, \cdots, a_n$，因此是 $\mathfrak{A}'$ 的一个眞包集合并且是 $\mathfrak{A}'$ 的一个单值象．根据归納假設这是不可能的．

由这条定理首先推出，一个集合不可能同时与自然数序列的两个不同的截段等势；否则这两个截段就相互等势，而其中一定有一个是另一个的眞包集合．因此一个有限集合 $\mathfrak{A}$ 只能与自然数序列的一个截段 $(1, n)$ 等势．这个唯一决定的数 n 称为集合 $\mathfrak{A}$ 的**元素的个数**，它可以作为集合的势的一个度量．

其次，由定理推出，自然数序列的一个截段不可能与整个自然数序列等势．因此自然数的序列是无穷的．与自然数序列等势的集合称为**可数无穷的**．可数无穷集合的元素可以用自然数来編号，在編号中每个自然数恰用到一次．

有限的与可数无穷的集合統称为可数的.

习题. 2. 証明. 两个不相交的有限集合的并的元素的个数等于这两个集合元素个数的和. [利用§3中递归公式(1), (2)作完全归納法.]

3. 証明: r 个两两不相交的元素个数为 s 的集合的并的元素个数为 rs. [利用§3中递归公式(6), (7)作完全归納法.]

4. 証明:自然数序列的每一个子集合都是可数的. 由此推知,一集合是可数的当且仅当它的元素可以用自然数編号,不同的元素有不同的号碼.

不可数集合的例子. 所有由自然数組成的可数无穷序列的集合不是可数的. 显然这个集合不是有限的. 假設它是可数无穷的,那么每个序列就有一个号碼,号碼为 i 的序列記为

$$a_{i1}, a_{i2}, \cdots.$$

我們現在作一个序列

$$a_{11}+1, a_{22}+1, \cdots.$$

这个序列一定也有一个号碼,譬如說是 j. 于是就有

$$a_{j1}=a_{11}+1; \quad a_{j2}=a_{22}+1; \quad 等等.$$

特别地

$$a_{jj}=a_{jj}+1,$$

这是一个矛盾.

习题. 5. 証明:整数(正的和負的和零)的集合是可数无穷的. 同样,偶数的集合是可数无穷的.

6. 証明:所有实数(也就是所有的无穷小数)的集合是不可数的. [証明的方法与上面例子中所用的方法相仿.]

7. 証明: 一个可数无穷集合的勢不因添加进去有限多个或者可数无穷多个元素而改变.

可数多个可数集合的并还是可数的.

証明. 設所給的集合为 $\mathfrak{M}_1, \mathfrak{M}_2, \cdots$; $\mathfrak{M}_i$ 的元素为 $m_{i1}, m_{i2}, \cdots$.

适合条件 $i+k=2$ 的元素 m_{ik} 只有有限多个, 同样, 适合

$i+k=3$ 的元素也只有有限多个，等等．首先我們把适合条件 $i+k=2$ 的元素加以編号（譬如按 i 的上升順序），然后把适合 $i+k=3$ 的元素編号，这样一直下去，最后每个元素 m_{ik} 都有了号碼，并且不同的元素有不同的号碼．由此即得結論．

习題． 8．証明：所有不可約分数 $\frac{\pm a}{b}$（a, b 是互素的自然数）的集合是可数无穷的．

§5. 分 类

等号适合以下的規則：

$$a=a.$$

由 $a=b$ 推出 $b=a$.

由 $a=b$ 与 $b=c$ 推出 $a=c$.

我們把上面的情形說成：关系 $a=b$ 是**自反的**，**对称的**与**传递的**．如果在某一集合的元素之間定义了一个关系 $a\sim b$（对于每两个元素 a, b 或者是 $a\sim b$ 或者不是）并且它适合同样的公理：

1. $a\sim a$;

2. 由 $a\sim b$ 推出 $b\sim a$;

3. 由 $a\sim b$ 与 $b\sim c$ 推出 $a\sim c$,

那么我們就称关系 $a\sim b$ 为一**等价关系**．例如，在§2 中对于集合 $\mathfrak{M}$, $\mathfrak{N}$, $\cdots$ 定义的关系 $\mathfrak{M}\sim\mathfrak{N}$（$\mathfrak{M}$ 与 $\mathfrak{N}$ 等势）就适合这些公理．又如三角形的全同关系也是这样一种关系．第三个例子：在整数中我們称两个数是等价的，如果它們的差能被 2 除尽．这些公理显然是适合的．

如果任給一个等价关系，那么我們就可以把全部与某一元素 a 等价的元素合并成一类 $\mathfrak{K}_a$．于是同一类中的元素必相互等价，因为由 $a\sim b$ 与 $a\sim c$ 根据 2. 与 3. 即得 $b\sim c$，并且所有与类中

一个元素等价的元素全属于同一类，因为由 $a \sim b$ 与 $b \sim c$ 推出 $a \sim c$。每一类由其中任一个元素决定：如果代替元素 a 我們給出 $\mathfrak{K}_a$ 中另一个元素 b，那么我們得到同一类：$\mathfrak{K}_a = \mathfrak{K}_b$。因此类中每一个元素 b 都可以选作这个类的**代表**。

但是，如果我們从不属于同一类的元素 b 出发(即 b 不与 a 等价)，那么 $\mathfrak{K}_a$ 与 $\mathfrak{K}_b$ 不可能有共同的元素；因为由 $c \sim a$ 与 $c \sim b$ 就要推出 $a \sim b$，从而 $b \in \mathfrak{K}_a$。因此在这个情形，类 $\mathfrak{K}_a$ 与 $\mathfrak{K}_b$ 不相交。

这些类蓋满了整个的集合，因为每个元素 a 都属于一类，即 a 在 $\mathfrak{K}_a$ 中。因此，集合被**分成了两两不相交的类**。在上面举的最后一个例子中，分成的两类是奇数与偶数。

我們看到，$\mathfrak{K}_a = \mathfrak{K}_b$ 当且仅当 $a \sim b$。如果引入类来代替元素，那么我們就可以把等价关系 $a \sim b$ 变成相等关系 $\mathfrak{K}_a = \mathfrak{K}_b$。

反过来，如果一个集合 $\mathfrak{M}$ 被分成了两两不相交的类，那么我們可以定义：$a \sim b$ 当 a, b 属于同一类。关系 $a \sim b$ 显然适合公理 1, 2, 3。

§6. 有序集合

以下三节在初次閱讀时可以略去不讀。它們包含那些在域的无限扩张理論(第八章)中要用到的关于集合的序与良序的一般定理。

一个集合称为**有序的**，如果对于它的元素定义了一个关系 $a < b$，适合

1. 对于任意两个元素 a, b，$a < b$ 或者 $b < a$ 或者 $a = b$；

2. 关系 $a < b$，$b < a$，$a = b$ 是互相排斥的；

3. 由 $a < b$ 与 $b < c$ 推出 $a < c$。

如果只要求性质 2. 与 3.，那么这个集合就称为偏序的. 格論討論这种偏序集合. 关于这方面的結果可以看 G. Birkhoff 的书 "Lattice Theory"（格論）（Amer. math. soc. colloq. publ.，25 卷，第二版，New York，1948）.

关系 $a<b$ 不一定是眞正的大小关系（如整数中的关系 $a<b$），它可以是用任意方法定义的；但是对任意两个元素 a，b 必須或者是 $a<b$ 或者不是. 例如，当一个集合的元素被排成一个序列，$a<b$ 就定义为 a 排在 b 之前，这个集合就有序了.

由关系 $a<b$ 我們定义一些导出关系：

$a>b$ 就是 $b<a$；

$a\leqslant b$ 就是：$a=b$ 或者 $a<b$；

$a\geqslant b$ 就是：$a=b$ 或者 $a>b$.

因此 $a\leqslant b$ 就等价于 $a>b$ 的否定，同样，$a\geqslant b$ 等价于 $a<b$ 的否定.

当 $a<b$，我們就說 a 在 b 之前，b 在 a 之后，也称 a 先于 b.

一个集合可能有一个"初始元素"，它先于所有其余的元素. 例：在自然数序列中的 1.

如果一个集合是有序的，那么对于同样的关系 $a<b$，它的每一个子集合也都是有序的.

一个有序集合称为良序的，如果它的每个非空子集合（特别这个集合本身）都有一个初始元素.

例.

1. 每个有限的有序集合是良序的（参看下面的习题 1）.

2. 自然数序列 1, 2, 3, ⋯ 是良序的，因为每个自然数的非空集合都有一初始元素.

3. 全体整数的集合 ⋯，−2，−1，0，1，2，⋯ 在"自然"順

序下不是良序的；因为它沒有初始元素． 但是如果給以另外的順序，它可能变成良序的，譬如

$$0, 1, -1, 2, -2, \cdots$$

或者

$$1, 2, 3, \cdots; \quad 0, -1, -2, -3, \cdots.$$

这里是把正数排在前面，其余的数就按絕对值的大小来排．

习題． 1．証明：在每个有序的非空有限集合中都有一初始元素．

2．对于自然数偶 (a, b) 所成的集合中按以下的方法定义一个顺序关系：$(a, b) < (a', b')$ 当 $a < a'$ 或者 $a = a', b < b'$．証明：这样定义了一个良序．

3．証明：在每个良序集合中每个元素 a（除去这个集合的最后元素，如果有的話）都有一个"直接后繼" $b > a$，这就是說，沒有元素 x 在 a 与 b 之間（即 $b > x > a$）．是否每个元素（除去初始元素）也都有一个直接先行？

§7. 选择公理与良序定理

Zermelo 第一个注意到許多数学的討論依賴于一个假設，他第一个明白地叙述了这个假設并称之为选择公理．它是：

对于由非空集合組成的任一个集合，都存在一"选择函数"，这就是說，它是使这些集合中的每一个都对应于它的一个元素的函数．

应該注意，这里假定了每个单个集合是非空的，因之由每个集合中一定能选出一个元素． 这个公理所肯定的是，由所有这些集合中可以按照一个对应規則同时作出选择．

以后在必要时，我們总是認为选择公理是成立的．

选择公理的最重要的推論是 Zermelo 的良序定理：

每个集合都是可以良序的．

Zermelo 曾对这个定理給出两个証明[1]；这里給的是他的第二个証明。

为了扼要地指出証明的要点，設想已經引入了一个良序。每个元素 a 决定一个"截段" $\mathfrak{A}(a)$（由所有 $< a$ 的元素組成）以及一个"余集" $\mathfrak{R}(a)$（由所有 $\geqslant a$ 的元素組成）。在証明中首先造出余集 $\mathfrak{R}(a)$ 的集合，作法是利用选择公理在 $\mathfrak{M}$ 的所有子集合中都指定一个元素，使得 a 恰好就是 $\mathfrak{R}(a)$ 中指定的那个元素，余集显然有以下性质：由 $\mathfrak{R}(a)$ 中除去 a 所得的集合还是一个余集（即 a 的后面一个元素的余集）。同样，任意多个余集的交还是一个余集。給定的集合 $\mathfrak{M}$ 本身也是余集。最后，如果 $\mathfrak{R}(a)$ 与 $\mathfrak{R}(b)$ 是两个不同的余集，那么 $\mathfrak{R}(a) \subset \mathfrak{R}(b)$ 或者 $\mathfrak{R}(a) \supset \mathfrak{R}(b)$（按照 $a > b$ 或者 $a < b$）。下面首先来构造具有这些性質的子集合的集合。

$\mathfrak{M}$ 的子集合以下記为 $\mathfrak{A}, \mathfrak{B}, \cdots$.

利用选择公理，我們首先使 $\mathfrak{M}$ 的每个非空子集合 $\mathfrak{A}$ 与一个"指定元素" a 对应。用 $\mathfrak{A}'$ 表示由 $\mathfrak{A}$ 中除去 a 所得的集合。在整个証明中"$'$"都表示这个意思。

$\mathfrak{M}$ 的子集合的一个集合 $\mathbf{K}$ 称为一个 Θ-鏈，如果具有以下的性質：

1. $\mathfrak{M}$ 本身属于 $\mathbf{K}$.

2. 如果 $\mathfrak{A}$ 属于 $\mathbf{K}$ 并且是非空的，那么 $\mathfrak{A}'$ 也属于 $\mathbf{K}$.

3. 如果集合 $\mathbf{A} = \{\mathfrak{A}, \mathfrak{B}, \cdots\}$ 中的元素 $\mathfrak{A}, \mathfrak{B}, \cdots$ 全属于 $\mathbf{K}$，那么交 $\mathfrak{D}(\mathbf{A})$ 也属于 $\mathbf{K}$.

Θ-鏈是存在的，譬如 $\mathfrak{M}$ 的所有子集合的集合就是。許多 Θ-鏈的交显然还是一个 Θ-鏈。因之所有 Θ-鏈的交 $\triangle$ 是一个 Θ-鏈。$\triangle$ 显然是一个极小的 Θ-鏈；这就是說，$\triangle$ 的眞子集合就不再是 Θ-鏈了。

在鏈 $\triangle$ 中我們特别考虑这样一种集合 $\mathfrak{A}$，鏈中所有其余的集合或者是 $\mathfrak{A}$ 的包集合，或者是 $\mathfrak{A}$ 的子集合。后面我們将証明，鏈中所有的集合都有这个性質；但是現在我們只知道，$\mathfrak{M}$ 是有这个性質的。在鏈中 $\mathfrak{A}$ 的眞包集合記为 $\mathfrak{O}_{\mathfrak{A}}$，眞子集合記为 $\mathfrak{U}_{\mathfrak{A}}$。如果一个 $\mathfrak{U}_{\mathfrak{A}}$ 甚至是 $\mathfrak{A}'$ 的子集合，那么我們記为 $\mathfrak{B}_{\mathfrak{A}}$.

对于一个固定的 $\mathfrak{A}$，所有的 $\mathfrak{O}_{\mathfrak{A}}$ 与 $\mathfrak{B}_{\mathfrak{A}}$ 与 $\mathfrak{A}$ 合起来也是一个 Θ-鏈；因为

a) $\mathfrak{M}$ 是一个 $\mathfrak{O}_{\mathfrak{A}}$ 或者就等于 $\mathfrak{A}$;

b) 每个由一个 $\mathfrak{O}_{\mathfrak{A}}$ 导出的集合 $(\mathfrak{O}_{\mathfrak{A}})'$ 或者还是一个 $\mathfrak{O}_{\mathfrak{A}}$ 或者就等于

---

1) *Math. Ann.*, **59** (1904), 514; *Math. Ann.*, **65** (1908), 107.

$\mathfrak{A}$. 否則，它(作为△的一个元素)必須是$\mathfrak{A}$的子集合，甚至是眞子集合。因之在$\mathfrak{A}$中有一个不属于$(\mathfrak{D}_\mathfrak{A})'$的元素。此外，在$\mathfrak{D}_\mathfrak{A}$中有一个不属于$\mathfrak{A}$的元素，它当然也不属于$(\mathfrak{D}_\mathfrak{A})'$。这样，在$\mathfrak{D}_\mathfrak{A}$中就有两个不同的元素不属于$(\mathfrak{D}_\mathfrak{A})'$，这与$(\mathfrak{D}_\mathfrak{A})'$的定义不符。

c) $\mathfrak{A}'$以及每个$\mathfrak{B}_\mathfrak{A}$都属于△，它們都是$\mathfrak{A}'$的子集合，因之都是$\mathfrak{B}_\mathfrak{A}$.

d) 許多$\mathfrak{D}_\mathfrak{A}$的交以及$\mathfrak{D}_\mathfrak{A}$与$\mathfrak{A}$的交还是$\mathfrak{A}$的包集合并且属于△，因之还是$\mathfrak{D}_\mathfrak{A}$或者$\mathfrak{A}$.

e) 許多$\mathfrak{B}_\mathfrak{A}$的交以及它們与$\mathfrak{D}_\mathfrak{A}$或者$\mathfrak{A}$的交都是$\mathfrak{A}'$的子集合并且属于△，因之还是$\mathfrak{B}_\mathfrak{A}$.

这样就証明了鍊性质。

但是因为△是一个极小Θ-鍊，所以$\mathfrak{D}_\mathfrak{A}$，$\mathfrak{B}_\mathfrak{A}$以及$\mathfrak{A}$合起来就是整个的△。从而每个$\mathfrak{U}_\mathfrak{A}$都是$\mathfrak{B}_\mathfrak{A}$，因为它既不是$\mathfrak{A}$又不是$\mathfrak{D}_\mathfrak{A}$.

由此推知，$\mathfrak{A}'$也具有我們假定$\mathfrak{A}$所具有的性质，即△中所有其余的集合不是$\mathfrak{A}'$的包集合，就是$\mathfrak{A}'$的子集合。

設集合$\mathfrak{A}$, $\mathfrak{B}$, … 都有上面所假定的性质，$\mathfrak{D}$是它們的交，而$\mathfrak{X}$是鍊△中另外一个集合，于是只可能有两种情形：$\mathfrak{X}$包含集合$\mathfrak{A}$, $\mathfrak{B}$, …中的一个从而$\mathfrak{X}$包含它們的交$\mathfrak{D}$，或者$\mathfrak{X}$包含在所有$\mathfrak{A}$, $\mathfrak{B}$, …之中从而$\mathfrak{X}$也包含在$\mathfrak{D}$之中。因之$\mathfrak{D}$也具有所說的性质。

最后，因为$\mathfrak{M}$本身具有所說的性质，所以△中所有具有这个性质的集合組成一Θ-鍊。因为△是极小的，所以这个鍊就是△。因之△的每个集合都具有所說的性质，即对于△中任意两个集合$\mathfrak{A}$, $\mathfrak{B}$必有$\mathfrak{A} \subseteq \mathfrak{B}$或者$\mathfrak{B} \subseteq \mathfrak{A}$.

現在設$\mathfrak{P}$是$\mathfrak{M}$的任一个非空子集合，$\mathfrak{P}_0$是△中所有包含$\mathfrak{P}$的集合(其中包括$\mathfrak{M}$)的交。$\mathfrak{P}_0$也属于△。$\mathfrak{P}_0$的指定元素p_0一定属于$\mathfrak{P}$，否則$\mathfrak{P}_0'$(由$\mathfrak{P}_0$除去元素p_0所得的集合)就包含$\mathfrak{P}$，而$\mathfrak{P}_0'$也属于△但是$\mathfrak{P}_0$的一个部分。△中其余的包含$\mathfrak{P}$的集合$\mathfrak{P}_1$一定包含$\mathfrak{P}_0$: $\mathfrak{P}_0$是每一个$\mathfrak{P}_1$的眞子集合。由前面的証明可知，$\mathfrak{P}_0$甚至是由$\mathfrak{P}_1$除去指定元素p_1所得的集合$\mathfrak{P}_1'$的子集合。因此p_1不在$\mathfrak{P}_0$中，当然也不在$\mathfrak{P}$中。在△中只有一个集合$\mathfrak{P}_0$，它包含$\mathfrak{P}$同时它的指定元素在$\mathfrak{P}$中。

如果我們取$\mathfrak{P} = \{a\}$，这里a是$\mathfrak{M}$中任意一个元素，那么就有，对于$\mathfrak{M}$中每一个元素a都有△中一个集合与之对应，这个集合的指定元素就是a。我們称这个集合为$\mathfrak{R}(a)$.

如果我們再取$\mathfrak{P} = \{a, b\}$，那么$\mathfrak{P}_0$的指定元素是a或者b；这就是說，

$\mathfrak{P}_0 = \mathfrak{R}(a)$ 或者 $\mathfrak{P}_0 = \mathfrak{R}(b)$. 二者不可能同时成立，否则指定元素就要既是 a 又是 b. 因之情形 $\mathfrak{R}(a) = \mathfrak{R}(b)$ 不可能，剩下只有 $\mathfrak{R}(a) \subset \mathfrak{R}(b)$ 与 $\mathfrak{R}(b) \subset \mathfrak{R}(a)$ 这两个可能性. 在第一个情形我們令 $b < a$,在第二个情形令 $a < b$.

根据以上証明，三个可能性

$$a < b, \quad a = b, \quad b < a$$

中一定有一个且只有一个出现. 传递律是成立的；因为由

$$\mathfrak{R}(c) \subset \mathfrak{R}(b), \quad \mathfrak{R}(b) \subset \mathfrak{R}(a)$$

推出

$$\mathfrak{R}(c) \subset \mathfrak{R}(a).$$

因此，关系 $a < b$ 定义了 $\mathfrak{M}$ 的一个序.

为了証明这是一个良序，我們来看 $\mathfrak{M}$ 的一个非空子集合 $\mathfrak{P}$ 以及 Δ 中对应的集合 $\mathfrak{P}_0$，它的指定元素 p_0 在 $\mathfrak{P}$ 中. 如果 p 是 $\mathfrak{P}$ 中任意一个元素，那么由于 $\mathfrak{R}(p)$ 是 Δ 中所有包含 p 的集合的交，而 $\mathfrak{P}_0$ 是 Δ 中一个这样的集合，所以

$$\mathfrak{R}(p) \subseteq \mathfrak{P}_0 = \mathfrak{R}(p_0),$$

从而

$$p_0 \leqslant p.$$

因之 p_0 是 $\mathfrak{P}$ 的初始元素，这就証明了全部結論.

良序的重要性在于，以前我們对于可数集合所知道的完全归納的方法可以推广到任意良序的集合. 这一点将在下一节討論.

§ 8. 超限归納法

超限归納証明法. 为了証明一个良序集合的元素全具有性質 E，我們可以这样进行：我們証明，只要一个元素的所有先行元素全具有性質 E，这个元素就具有性質 E（特别这个集合的初始元素具有性質 E）. 于是所有的元素就都具有性質 E. 因为假如有元素不具有性質 E，那么在这些元素中有一个初始元素 e，但是它的所有先行元素都具有性質 E，从而 e 也具有，这就得出一个矛

盾。

超限归納构造法. 假如我們要使良序集合 $\mathfrak{M}$ 中每个元素 x 都与一个新的对象 $\varphi(x)$ 对应，为了决定这个对应，我們給了一个关系，即所謂"递归定义关系"，它把函数值 $\varphi(a)$ 与函数值 $\varphi(b)$ $(b < a)$ 联系起来. 假定一旦所有的函数值 $\varphi(b)(b < a)$ 給定之后，这个关系就唯一地决定函数值 $\varphi(a)$，它們一齐适合所給的关系，当然也可以是一組关系而不是一个关系.

定理. *在所作的假定之下，有一个且只有一个函数 $\varphi(x)$ 适合所給的关系.*

首先来証唯一性. 假設有两个不同的函数 $\varphi(x)$，$\psi(x)$，它們都适合定义关系. 一定有一个初始的 a 使 $\varphi(a) \neq \psi(a)$. 对于所有的 $b < a$，有 $\varphi(b) = \psi(a)$. 根据假定，一旦所有的 $\varphi(b)$ 給定之后，关系就唯一地决定函数值 $\varphi(a)$，从而 $\varphi(a) = \psi(a)$，与假設冲突.

为了証明存在，我們考虑集合 $\mathfrak{M}$ 的截段 $\mathfrak{A}$（截段 $\mathfrak{A}$ 就是所有先于一个元素 a 的元素的集合）. 它們組成（以关系 $\mathfrak{A} \subset \mathfrak{B}$ 作为順序关系）一良序集合；因为每个元素 a 1-1 地与一个截段 $\mathfrak{A}$ 相对应，由 $b < a$ 推出 $\mathfrak{B} \subset \mathfrak{A}$. 如果我們取集合 $\mathfrak{M}$ 本身作为最后一个截段，那么这个集合仍然是良序的.

我們現在对 $\mathfrak{A}$ 作归納来証明，在每个集合 $\mathfrak{A}$ 上都存在一个函数 $\varphi(x) = \varphi_{\mathfrak{A}}(x)$（对于 $\mathfrak{A}$ 中所有 x 定义），适合所給的关系. 假定对于所有先于截段 $\mathfrak{A}$ 的截段結論已証. 有两个情形：

1. $\mathfrak{A}$ 有一个最后的元素 a. 在由 $\mathfrak{A}$ 除去元素 a 所得的集合 $\mathfrak{A}'$ 上已經定义了函数 $\varphi(x)$，因为 $\mathfrak{A}'$ 是先于 $\mathfrak{A}$ 的截段. 根据定义关系由全体函数值 $\varphi(b)(b < a)$ 唯一地定义 $\varphi(a)$. 加进这个函数值，函数 φ 就对于 $\mathfrak{A}$ 的所有元素都定义了，并且适合定义关系.

2. $\mathfrak{A}$ 沒有最后的元素. $\mathfrak{A}$ 的每个元素 a 因之都属于前面的某一个截段 $\mathfrak{B}$. 在前面的每个截段 $\mathfrak{B}$ 上都已經定义了一个函数 $\varphi_{\mathfrak{B}}$. 我們希望定义:

$$\varphi(a) = \varphi_{\mathfrak{B}}(a),$$

为此首先必須証明,这些属于不同截段的函数 $\varphi_{\mathfrak{B}}, \varphi_{\mathfrak{C}}, \cdots$ 在这些截段的每个公共的点上有相同的值. 假設 $\mathfrak{B}$ 与 $\mathfrak{C}$ 是不同的截段并且 $\mathfrak{B} \subset \mathfrak{C}$. 于是 $\varphi_{\mathfrak{B}}$ 与 $\varphi_{\mathfrak{C}}$ 在 $\mathfrak{B}$ 上都定义并且都适合所給的关系;因此它們重合(根据已經証明的唯一性). 因之定义 $\varphi(a) = \varphi_{\mathfrak{B}}(a)$ 是有意义的. 显然这样造出的函数 φ 适合定义关系,因为所有的函数 $\varphi_{\mathfrak{B}}$ 全适合.

不論是情形 1 还是情形 2, 在 $\mathfrak{A}$ 上都有一个函数 φ 具有給定的性質,这样就証明了在每一个截段上函数的存在. 如果特别就取集合 $\mathfrak{M}$ 本身作为一个截段,那么結論就証明了.

第二章　羣

內容. 本章中闡述了作为全书基础的几个羣論基本概念：羣、子羣、同构、同态、正規子羣和商羣.

§9. 羣的概念

定义. 由任意某种元素（如数、映射、变換等）組成的一个非空集合 $\mathfrak{G}$ 称为一个羣，如果下列条件成立：

1. 給定了一个运算法则，对于集合 $\mathfrak{G}$ 中的每对元素 a 和 b，都有集合中的第三个元素与之对应，这个元素通常称为 a 和 b 的积，記作 ab 或 $a\cdot b$（两个元素的积可能和因子的次序有关，即不一定有 $ab=ba$）.

2. 結合律. 对 $\mathfrak{G}$ 中的任意三个元素 a, b, c，等式

$$ab\cdot c = a\cdot bc$$

成立.

3. $\mathfrak{G}$ 中存在（至少）一个（左）单位元素 e，它具有下列性质：对 $\mathfrak{G}$ 中所有元素 a

$$ea = a.$$

4. 对 $\mathfrak{G}$ 中每个元素 a，$\mathfrak{G}$ 中存在（至少）一个（左）逆元素 a^{-1}，它具有性質

$$a^{-1}a = e,$$

在这个等式中，出現于右端的总是同一个（左）单位元素 e.

一个羣称为 Abel 羣，如果除了以上各点之外还有 $ab=ba$（交

换律)成立.

例. 如果集合中的元素是数,而运算法则是普通的乘法,那末首先应該把零这个数除外,它是沒有逆元素的. 这时所有不等于零的有理数形成一个羣(单位元素是数 1);同样数 1 和 -1 形成一个羣,单独一个数 1 也形成羣.

羣的概念和所采用的表記方式无关:基本运算法則也可以是数的加法,只要規律 1. 至 4. 成立即可. 这时只須改变一下两个元素 a 和 b 相結合时所得第三元素的名称,不把它叫做"积",而在所有运算規律中把"积 $a \cdot b$"的字样改讀为"和 $a+b$"就行. 在这一情形下,数 0 是单位元素,因为对所有的数 a 有 $0+a=a$. 同样,数 $-a$ 是数 a 的逆元素,因为我們有 $-a+a=0$. 对于数来說,加法的結合律:

$$a+(b+c)=(a+b)+c$$

是永远成立的. 因此,如果一个数集在包含任意二数 a 和 b 的同时也包含着它們的和,并且它包含数零,而在包含每个数 a 的同时也包含着与之异号的数 $-a$,那末这个数集对加法来說形成一个羣. 这样一种数集也称为数模. 举例来說,有理数的全体形成一个模. 同样,整数的全体与偶数的全体形成模. 最后,单独一个数 0 也形成模.

平面繞着一个固定点的一切旋轉的全体,乃是羣的另一个例子,这个羣的元素不再是数. 将旋轉 A 和 B 相結合,就是一个接着一个地作出这两个旋轉. 先作旋轉 B,再作旋轉 A,其效果可以通过一个单独的旋轉来实現,这个旋轉我們就記作 $A \cdot B$ 或 AB. 結合律成立这一事实,在下面将要作为任意变换的結合律的一个特殊情形給出. 旋轉羣中的单位元素即角度为 0 的旋轉,这个旋轉使得每个点都不动. 一个給定旋轉的逆元素就是和它相反的旋

轉，这个旋轉刚好抵消前者的作用.

平面旋轉羣是一个 Abel 羣. 可是如果我們把相对于通过一固定点的所有直綫的反射也添加进去，那就会得出一个非 Abel 羣. 先作反射 A 再作反射 B，或者先作反射 B 再作反射 A，其效果是互不相同的.

这两个羣可以归結到**变换羣**的一般概念中去. 所謂集合 $\mathfrak{M}$ 的一个**变换**或**置换**，指的就是集合 $\mathfrak{M}$ 到它自身之上的一个 1-1 映射，即那样一个对应 s，在这个对应之下，$\mathfrak{M}$ 中的每个元素 a 都有一个象元素 $s(a)$ 与之相当，并且 $\mathfrak{M}$ 中的每个元素恰是一个元素 a 的象. $s(a)$ 也可以写成 sa. $\mathfrak{M}$ 中的元素是变换 s 的作用**对象**. 变换一詞通常用于无限集合，而置换一詞則通常用于有限集合.

如果集合 $\mathfrak{M}$ 是有限的，并且它的元素都已編好了号碼 $1, 2, \cdots, n$，那末它的每个置换都可以用一个图式完全表达出来；在这个图式中，每个号碼 k 的下方写着象元素的号碼 $s(k)$. 例如

$$s=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 3 & 1\end{pmatrix}$$

就是数碼 1, 2, 3, 4 的那样一个置换，它把 1 换成 2，2 换成 4，3 换成 3，而把 4 换成 1.

两个变换 s, t 的**积** st，就是先作变换 t 然后再对象元素作变换 s 所得出的那个变换[1)]，即

$$st(a)=s(t(a)).$$

例如，当 $s=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 3 & 1\end{pmatrix}$，$t=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}$ 时，我們有

1) 因子的次序完全是約定的. 經常可以看到恰恰相反的記法. 这时 st 的意义是：先作 s，再作 t. 采用这种記法时，将变换写在作用对象的右边，即把 $s(a)$ 写成 as，要来得更方便.

$$st = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \text{ 而 } ts = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

对变换来說，結合律：

$$(rs)t = r(st)$$

可以一般地証明如下：将上式两端作用于任意对象 a 有

$$(rs)t(a) = (rs)(t(a)) = r(s(t(a))),$$
$$r(st)(a) = r(st(a)) = r(s(t(a))).$$

因而两次都得到同一結果.

单位变换就是那样一个变换 I，它把每个对象都映射成它自身：

$$I(a) = a.$$

单位变换显然具有羣中单位元素的特性，即对任意变换 s 有 $Is = s$.

变换 s 的逆变换就是那样一个变换，它把 $s(a)$ 映射成为 a，从而抵消 s 的作用．我們把逆变换記作 s^{-1}，这样一来，对任意对象 a 有

$$s^{-1}s(a) = a,$$

因而有

$$s^{-1}s = I.$$

从以上所証可以看出，对集合 $\mathfrak{M}$ 的全部置换来說，公設 1. 至 4. 都满足．因此这些置換的全体形成一个羣．当 $\mathfrak{M}$ 为具有 n 个元素的有限集合时，它的全部置換所組成的羣也称为对称羣 $\mathfrak{S}_n$[1].

除此之外还可以看出，由 $\mathfrak{M}$ 的某些变换所組成的集合 $\mathfrak{G}$ 是一个羣，只要这个集合：a) 在包含任意两个变换的同时也包含着

1) 变量 $x_1, x_2, \cdots, x_n$ 的函数，在 $\mathfrak{S}_n$ 中所有置換下不变者称为"对称函数"．对称羣这个名称的来源就在于此．

它們的积；b) 在包含每个变换的同时也包含着它的逆变换；c) 包含单位变换. 如果集合 $\mathfrak{G}$ 是非空的，那末連 c) 这一要求也是多余的，因为如果 s 是 $\mathfrak{G}$ 中任一变换，那末根据 b)，s^{-1} 属于集合 $\mathfrak{G}$，因而根据 a)，$s^{-1}s = I$ 也属于 $\mathfrak{G}$.

現在让我們再回到羣的一般理論上来.

$ab\cdot c$ 或 $a\cdot bc$ 可簡写作 abc.

由 3. 和 4. 可知

$$a^{-1}aa^{-1} = ea^{-1} = a^{-1}.$$

左乘 a^{-1} 的一个逆元素即得

$$eaa^{-1} = e,$$

或

$$aa^{-1} = e.$$

因此每一个左逆元素同时也是一个右逆元素. 同时还可看到，a^{-1} 的一个逆元素是 a. 其次，从这里还可得出

$$ae = aa^{-1}a = ea,$$

因此左单位元素同时也是右单位元素.

現在还可以推出羣中的(两側)可除性.

5. 方程 $ax = b$ 在 $\mathfrak{G}$ 中有一个解；同样，方程 $ya = b$ 也在 $\mathfrak{G}$ 中有一个解，这里 a 和 b 是 $\mathfrak{G}$ 中的任意元素.

这两个解是 $x = a^{-1}b$, $y = ba^{-1}$，因为我們有

$$a(a^{-1}b) = (aa^{-1})b = eb = b,$$

$$(ba^{-1})a = b(a^{-1}a) = be = b.$$

除法的唯一性也可以同样簡单地証明：

6. 由 $ax = ax'$，同样由 $xa = x'a$，可得出 $x = x'$.

由 $ax = ax'$ 两端左乘 a^{-1} 可得 $x = x'$. 完全同样可以証明断言中的第二部分.

特别，从这里可以推出单位元素(作为方程 $xa=a$ 的解)的唯一性以及逆元素(作为方程 $xa=e$ 的解)的唯一性。 羣中(唯一)的单位元素常常記作 1.

可除性条件 5. 可以作为一个公設来代替公設 3. 和 4.。 現在让我們假定 1., 2. 和 5. 成立，从而証明 3.。 我們取出一个元素 c 并将方程 $xc=c$ 的一个解看作 e. 这样便有

$$ec=c.$$

对于任意元素 a，我們解出方程

$$cx=a.$$

这时便有

$$ea=ecx=cx=a.$$

这就証明了 3.。 公設 4. 只不过是方程 $xa=a$ 的可解性的一个直接推論而已。

这样一来，我們就可以将 1., 2., 5. 当作和 1., 2., 3., 4. 等价的羣公設来运用。

如果 $\mathfrak{G}$ 是一个有限集合，那末 5. 还可以用 6. 来代替. 这样我們就可以不必假定除法的可能性(除公設 1. 和 2. 之外)，只須假定除法的唯一性就行了。

証明. 設 a 是任意一个元素. 对每个元素 x，我們使元素 ax 与之对应. 根据 6. 这一对应是双方单值的，也就是說，集合 $\mathfrak{G}$ 被 1-1 地映射成它的一个子集，即所有积 ax 的集合. 然而根据假定 $\mathfrak{G}$ 是一个有限集合，它不可能被一对一地映射成一个眞子集. 因此，元素 ax 的全体和集合 $\mathfrak{G}$ 相一致，也就是說，每个元素 b 都可表成 $b=ax$ 的形状. 这就是 5. 中第一項要求所断定的. 同样可以証明 $b=xa$ 的可解性. 这样一来，就由 6. 推出了 5.。

一个有限羣中元素的个数称为这个羣的阶。

进一步的运算規律. 关于积的逆元素，下面的規律成立：

$$(ab)^{-1} = b^{-1}a^{-1}.$$

事实上我們有

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}ab) = b^{-1}b = e.$$

在 Abel 羣的情形，将运算法則写成加法的形式，即不写 $a \cdot b$ 而写 $a + b$，經常是比較合适的. 这时我們把 Abel 羣称为加羣或模(这是前面所定义的数模的推广). 在这一情形下，单位元素記作 0，因为它和整数系統中的数零一样可由性質

$$0 + a = a$$

来刻划. 类似地，在一个模中元素 a 的逆元素記作 $-a$.

元素 $a + (-b)$ 可以簡写作 $a - b$，因为这个元素是方程 $x + b = a$ 的解：

$$(a - b) + b = a + (-b + b) = a + 0 = a.$$

习题. 1. 空間的欧基里德运动带上反射（即使得每两个点之間的距离不变的一切变换）組成一个非 Abel 羣.

2. 証明元素 e, a 对下列运算法則

$$ee = e, \quad ea = a, \quad ae = a, \quad aa = e$$

組成一个羣.

注. 我們可以用一个"羣表"把羣中的运算法則表示出来，在表格的最上一行和最左一列中写出了羣的元素，两个元素的积写在相应行和列的交叉位置上. 例如上面講到的这个羣的羣表是：

	e	a
e	e	a
a	a	e

3. 試列出三个数碼的全部置换所組成的羣的羣表.

多个元素的积与和、幂. 正好象我們曾經把积 $a \cdot bc$ 簡写作 abc 一样，現在我們要来定义多个因子的連乘积：

$$\prod_{\nu=1}^{n} a_\nu = \prod_{1}^{n} a_\nu = a_1 a_2 \cdots a_n.$$

假設已經給定了一組元素 $a_1, a_2, \cdots, a_N$. 对于 $n < N$ 我們用遞归的方式定义：

$$\begin{cases} \prod_{1}^{1} a_\nu = a_1 \\ \prod_{1}^{n+1} a_\nu = \left(\prod_{1}^{n} a_\nu\right) \cdot a_{n+1}{}^{1)}. \end{cases}$$

特别 $\prod_{1}^{3} a_\nu$ 就是我們已有了的 $a_1a_2a_3$. 同样, $\prod_{1}^{4} a_\nu = a_1a_2a_3a_4 = (a_1a_2a_3)a_4$, 等等。

現在我們可以仅仅利用結合律証明下面的規律：

$$\prod_{\mu=1}^{m} a_\mu \cdot \prod_{\nu=1}^{n} a_{m+\nu} = \prod_{\nu=1}^{m+n} a_\nu. \tag{1}$$

用文字表达出来就是說：两个連乘积的积等于它們的全部因子在原有次序下的連乘积. 例如：

$$(ab)(cd) = abcd$$

就是公式 (1) 的一个特例。

当 $n = 1$ 时，公式 (1) 是显然的(根据 Π-記号的定义). 假設这个公式对某一值 n 已經証明，那末对于下一个值 $n+1$ 将会有

$$\begin{aligned} \prod_{1}^{m} a_\mu \cdot \prod_{1}^{n+1} a_{m+\nu} &= \prod_{1}^{m} a_\mu \left(\prod_{1}^{n} a_{m+\nu} \cdot a_{m+n+1}\right) \\ &= \left(\prod_{1}^{m} a_\mu \cdot \prod_{1}^{n} a_{m+\nu}\right) a_{m+n+1} \\ &= \left(\prod_{1}^{m+n} a_\mu\right) a_{m+n+1} = \prod_{1}^{m+n+1} a_\nu. \end{aligned}$$

---

1) 表示变动足数的記号 ν 当然可以换成任意其它的記号而不改变連乘积本身的意义。

这样就証明了公式(1)。

注意。 連乘积 $\prod_{1}^{n} a_{m+\nu}$ 也可以写作 $\prod_{m+1}^{m+n} a_{\nu}$。在方便的情况下也可以命 $\prod_{1}^{0} a_{\nu} = e$。

n 个相同因子的积称为一个**冪**：

$$a^n = \prod_{1}^{n} a \text{（特别 } a^1 = a,\ a^2 = aa, \text{余类推）}.$$

由前面証明的定理可得

$$a^n \cdot a^m = a^{n+m}. \tag{2}$$

此外还可得出

$$(a^m)^n = a^{mn}. \tag{3}$$

这个公式的証明留給讀者自己(利用完全归納法)去完成。

到目前为止所建立起来的規律(1)，(2)，(3)，其証明中只用到結合律。因此这些規律在今后可以应用于各种不同的系統，只要在这些系統中定义了积的概念，并且結合律成立就行(例如自然数系)，即使它們不是羣也可以。

如果羣中的乘法是交換的(Abel 羣)，那末还可以进一步証明連乘积的值与因子的次序无关。更确切地說：如果 φ 是把自然数截段 $(1, n)$ 映成它自身的一个 1-1 映射，那末

$$\prod_{\nu=1}^{n} a_{\varphi(\nu)} = \prod_{1}^{n} a_{\nu}.$$

証明。 对于 $n=1$ 这个断言是显然的。現在假設它对 $n-1$ 成立。必定有一个 k 被映射成 n：$\varphi(k) = n$。这样便有

$$\prod_{1}^{n} a_{\varphi(\nu)} = \prod_{1}^{k-1} a_{\varphi(\nu)} \cdot a_{\varphi(k)} \cdot \prod_{1}^{n-k} a_{\varphi(k+\nu)} = \prod_{1}^{k-1} a_{\varphi(\nu)} \cdot \prod_{1}^{n-k} a_{\varphi(k+\nu)} \cdot a_{\varphi(k)}\text{[1]}.$$

1) 当 $k=1$ 时，第一个因子消失；当 $n=k$ 时第二个因子消失。可是这并不影响証明本身。

現在我們定义截段 $(1, n-1)$ 到它自身的一个映射 ψ 如下：

$$\psi(\nu)=\varphi(\nu) \quad (\nu<k),$$
$$\psi(\nu)=\varphi(\nu+1) \quad (\nu \geqslant k).$$

这样就可以得出

$$\prod_{1}^{n} a_{\varphi(\nu)}=\prod_{1}^{k-1} a_{\psi(\nu)} \prod_{1}^{n-k} a_{\psi(k-1+\nu)} \cdot a_{n}=\prod_{1}^{n-1} a_{\psi(\nu)} \cdot a_{n},$$

从而根据归納假設可知这个連乘积等于

$$\prod_{1}^{n-1} a_{\nu} \cdot a_{n}=\prod_{1}^{n} a_{n}.$$

根据上面証明的規律可知，对 Abel 羣来說，我們可以采用

$$\prod_{1 \leqslant i<k \leqslant n} a_{ik}$$

或

$$\prod_{i<k} a_{ik} \quad (i=1, \cdots, n; \quad k=1, \cdots, n)$$

这样的記法．这种記法的意义是說：可以将满足条件 $1 \leqslant i<k \leqslant$ $\leqslant n$ 的足数对 i, k 的集合排成任意次序，然后再相应地作出連乘积．

在任意羣中可以按通常方式定义一个元素 a 的零次冪和負冪：

$$a^{0}=1,$$
$$a^{-n}=\left(a^{-1}\right)^{n},$$

并很容易地証明，規律（2）和（3）現在对任意整指数成立．

在一个加羣中自然地应把 $\prod\limits_{1}^{n} a_{\nu}$ 写成 $\sum\limits_{1}^{n} a_{\nu}$，并把 a^{n} 相应地写成 $n \cdot a$．在整数加羣中，这一定义和两个整数的积的定义一致．对积所証明的一切結論，現在可以应用于和．

采用加法記号时，运算規則（3）具有結合律的形式：

$$n \cdot m a=n m \cdot a,$$

而(2)则具有"分配律"的形式：

$$ma + na = (m + n)a.$$

除此二者之外，还有另外一个分配律：

$$m(a + b) = ma + mb$$

[采用乘法記号时应为 $(ab)^m = a^m b^m$，但这个規律仅在 Abel 羣中成立]．利用归納法很容易証明这个公式．

习題． 4．証明对 Abel 羣来說，有

$$\prod_{\nu=1}^{n}\prod_{\mu=1}^{m} a_{\mu\nu} = \prod_{\mu=1}^{m}\prod_{\nu=1}^{n} a_{\mu\nu}.$$

5．同样

$$\prod_{\nu=1}^{n}\prod_{\mu=1}^{\nu} a_{\mu\nu} = \prod_{\mu=1}^{n}\prod_{\nu=\mu}^{n} a_{\mu\nu}.$$

6．对称羣 $\mathfrak{S}_n$ 的阶是 $n! = \prod\limits_{1}^{n} \nu$ [对 n 作完全归納法]．

§10. 子　　羣

羣 $\mathfrak{G}$ 的一个非空子集 $\mathfrak{g}$ ($\mathfrak{G}$ 中給定了的同一运算法則)形成一个羣的充分必要条件是，这个子集满足条件 1.，2.，3.，4．条件 1. 断言，如果 a 和 b 属于 $\mathfrak{g}$，则 ab 也属于 $\mathfrak{g}$．条件 2. 对 $\mathfrak{g}$ 自然成立，因为它即使对 $\mathfrak{G}$ 来說也是成立的．条件 3. 和 4. 断定，单位元素在 $\mathfrak{g}$ 内，并且 $\mathfrak{g}$ 在包含每个元素 a 的同时也包含着它的逆元素 a^{-1}．在这里关于单位元素的要求也是多余的，因为如果 a 是属于 $\mathfrak{g}$ 的任意元素，则 a^{-1} 也属于 $\mathfrak{g}$，因而积 $aa^{-1} = e$ 也属于 $\mathfrak{g}$．这样我們就証明了下面的結論：

羣 $\mathfrak{G}$ 中的一个非空子集 $\mathfrak{g}$ 是子羣的充分必要条件是：

1．$\mathfrak{g}$ 在包含任意两个元素 a 和 b 的同时也包含着它們的积 ab；

2. $\mathfrak{g}$ 在包含每个元素 a 的同时也包含它的逆元 a^{-1}.

特别，如果 $\mathfrak{g}$ 是有限子集，那末甚至連这里的第二項要求也是多余的；因为在这一情形下我們可以用 6. 来代替 3. 和 4.，而条件 6. 对 $\mathfrak{g}$ 来說是成立的，因为它即使对 $\mathfrak{G}$ 来說也成立。

一般地，我們可以把条件 1. 和 2. 合并成为一个条件：$\mathfrak{g}$ 在包含 a 和 b 的同时也包含着 ab^{-1}. 事实上，在这一条件下 $\mathfrak{g}$ 在包含元素 a 的同时必定包含元素 $aa^{-1}=e$，进一步可知它必包含元素 $ea^{-1}=a^{-1}$，因此它在包含 a 和 b 的同时也包含着 b^{-1} 和 $a(b^{-1})^{-1}=ab$。

当羣运算为加法运算(在 Abel 羣中)时，子羣可由下面的事实来刻划，即它在包含 a 和 b 的同时也包含着 $a+b$，在包含 a 的同时也包含着 $-a$。 这两个条件也可以用一个条件来代替，即子羣在包含 a 和 b 的同时也包含着 $a-b$.

子羣的例子.

每一个羣都以单位羣 $\mathfrak{E}$ 作为它們的子羣，这就是仅由单个的单位元素組成的子羣.

n 个对象的全部置換所組成的对称羣 $\mathfrak{S}_n$ 中，一个最重要的子羣就是交錯羣 $\mathfrak{A}_n$. 这个子羣是由所有那样一些置換組成的，当我們把这种置換作用于变元 $x_1, x_2 \cdots, x_n$ 时，函数

$$\Delta = \prod_{i<k}(x_i - x_k)$$

保持不变. 这种置換称为偶置換，其余的置換称为奇置換，后者改变函数 Δ 的符号. 每一个对換(即交換两个数碼的置換)都是奇置換. 两个偶置換或两个奇置換的积是偶置換，一个偶置換和一个奇置換的积是奇置換. 由第一个性质可知，$\mathfrak{A}_n$ 是一个羣. 由于一个固定的对換和一个偶置換相乘的积是奇置換，和奇置換相乘的

积是偶置换，故偶置换和奇置换是一样多的. 每种置换都是 $n!/2$ 个(参看 §9. 习题 6).

为了便于写出对称羣 $\mathfrak{S}_n$ 中的子羣起見，我們可以利用熟知的置换的輪換表示法：

我們用 $(pqrs)$ 表示一个輪換，它把 p 換成 q，q 換 r，r 換 s，s 換成 p，而使得所有其余的对象不变. 很容易証明，每一个置換都可以(除了因子的次序外)唯一地表成輪換或"循环"的乘积

$$(ikl\cdots)(pq\cdots)\cdots$$

的形式，使得其中沒有两个輪換含有相同的数碼. 这一乘积中的各个因子是彼此可交換的. 由一个数碼組成的循环，例如(1)，就是单位置換. 显然有

$$(1254) = (2541)$$

等等.

利用这样一种記法，我們可以把 $\mathfrak{S}_3$ 中的 $3! = 6$ 个置換表示如下：

$$(1),\ (12),\ (13),\ (23),\ (123),\ (132).$$

这个羣中的子羣也很容易确定出来(除 $\mathfrak{S}_3$ 本身之外)，它們是：

$\mathfrak{A}_3$: (1), (123), (132);

$\mathfrak{S}_2$: (1), (12);

$\mathfrak{S}_2'$: (1), (13); $\mathfrak{S}_2''$: (1), (23);

$\mathfrak{E}$: (1).

設 $a, b, \cdots$ 是羣 $\mathfrak{G}$ 中的任意一組元素，除了 $\mathfrak{G}$ 之外，可能还有别的子羣含着这些元素. 所有这些子羣的交是一个羣 $\mathfrak{A}$. 我們把这个羣称为由元素 $a, b, \cdots$ 所生成的羣. 这个羣显然包含一切可能的积，例如 $a^{-1}a^{-1}bab^{-1}\cdots$(每个积由有限多个因子构成，这些因子可以重复出現). 另一方面，这样一些乘积組成一个羣. 这个羣包含着元素 $a, b, \cdots$，因而包含着羣 $\mathfrak{A}$，因此后述的这个羣和羣 $\mathfrak{A}$ 重合. 这样，我們就証明了下面的結論：

由元素 $a, b, \cdots$ 所生成的羣是由所有那样的元素組成的，其中每个元素都可以表成有限多个生成元素及其逆元素的积.

特别，一个单独的元素 a 所生成的羣由所有的冪 $a^{\pm n}$ (包括

$a^0=e$)組成．由于

$$a^n a^m = a^{n+m} = a^m a^n,$$

这个羣是一个 Abel 羣．

由一个单独元素的一切冪所組成的羣称为**循环羣**．

这里可能出現两种不同的情况．或者所有的冪 a^h 都是互不相同的，这时循环羣

$$\cdots, a^{-2}, a^{-1}, a^0, a^1, a^2, \cdots$$

是**无限的**．或者可能出現

$$a^h = a^k, \quad h > k$$

的情形．这时我們有

$$a^{h-k} = e \qquad (h-k>0).$$

在这一情形下，我們令 n 为使得 $a^n=e$ 成立的最小正整数．冪 $a^0, a^1, a^2, \cdots, a^{n-1}$ 一定是互不相同的，因为由

$$a^h = a^k \qquad (0 \leqslant k < h < n)$$

將会得出

$$a^{h-k} = e \qquad (0 < h-k < n),$$

而这是和我們对 n 所作的假設相違背的．

每个整数 m 都可以表成

$$m = qn + r \qquad (0 \leqslant r < n)$$

的形式，因此

$$a^m = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = ea^r = a^r.$$

这就是說，a 的一切可能的冪都已經出現在叙列 $a^0, a^1, \cdots, a^{n-1}$ 中了．因此，我們所討論的循环羣恰有 n 个元素，即

$$a^0, a^1, \cdots, a^{n-1}.$$

数 n 乃是 a 所生成的羣的阶，这个数也就称为**元素 a 的阶**．如果 a 的各个冪互不相同，就称它为一个**无限阶元素**．

例. 整数

$$\cdots, -2, -1, 0, 1, 2, \cdots$$

以加法为运算法则組成一个无限循环羣. 前面講到过的羣 $\mathfrak{S}_2$, $\mathfrak{A}_3$ 是阶为 2 和 3 的循环羣.

习題. 1. 在一个 Abel 羣中一个 m 阶元素和一个 n 阶元素的积是一个 mn 阶元素，这里 m 和 n 是两个沒有大于 1 的公因子的整数.

2. 任給一正整数 n，証明存在着由置换組成的 n 阶循环羣.

3. 对 n 使用归納法証明：当 $n>1$ 时，$n-1$ 个对换 $(12), (13), \cdots, (1n)$ 生成对称羣 $\mathfrak{S}_n$.

4. 用同样的方法証明：当 $n>2$ 时，$n-2$ 个 3-循环 $(123), (124), \cdots, (12n)$ 生成交錯羣 $\mathfrak{A}_n$.

現在讓我們来决定一个循环羣的全部子羣. 設 $\mathfrak{G}$ 是由元素 a 所生成的循环羣，$\mathfrak{g}$ 是它的一个异于单位羣的子羣. 如果 $\mathfrak{g}$ 含有某一具有負指数的元素 a^{-m}，那末它的逆元素 a^m 也属于 $\mathfrak{g}$. 現在假設 a^m 是子羣 $\mathfrak{g}$ 中具有最小正指数的元素，我們証明 $\mathfrak{g}$ 中所有元素都是 a^m 的冪. 事实上，設 a^s 是 $\mathfrak{g}$ 中的任意一个元素，我們可命

$$s = qm + r \qquad (0 \leqslant r < m),$$

这时 $a^s(a^m)^{-q} = a^{s-mq} = a^r$ 将是 $\mathfrak{g}$ 中的一个元素，并且 $r<m$. 由于数 m 的选择方式，必有 $r=0$. 因此我們有 $s=qm$ 而 $a^s = (a^m)^q$. 这样，$\mathfrak{g}$ 中所有元素都是 a^m 的冪.

如果 a 具有有限阶 n，$a^n=e$，那末由于 $a^n=e$ 属于子羣 $\mathfrak{g}$，n 必能被 m 除尽：$n=qm$. 这样，子羣 $\mathfrak{g}$ 由元素 $a^m, a^{2m}, \cdots, a^{qm}=e$ 組成，其阶数为 q. 如果 a 是一个无限阶元素，則子羣 $\mathfrak{g}$ 由互不相同的元素 $e, a^{\pm m}, a^{\pm 2m}, \cdots$ 組成，因而也是无限的. 这样我們就証明了結論：

循环羣的子羣仍是循环羣. 它或者仅由单位元素組成，或者由具有最小可能正指数 m 的元素 a^m 的一切冪組成，換句話說，它

由原来那个循环羣中的元素的 m 次幂組成. 在无限循环羣的情形，m 可以是任意的，而在阶为 n 的有限循环羣的情形，m 必須是 n 的一个因子. 在后一情形子羣的阶数是 $q = n/m$. 相应于 n 的每一个因子 m，循环羣 $\{a\}$ 有一个而且仅有一个子羣 $\{a^m\}$.

§11. 羣子集的运算. 陪集

由羣 $\mathfrak{G}$ 中的元素所組成的任意集合称为羣子集.

两个羣子集 $\mathfrak{g}$ 和 $\mathfrak{h}$ 的积 $\mathfrak{g}\mathfrak{h}$ 就是所有乘积 gh 的集合，其中 g 取自 $\mathfrak{g}$ 而 h 取自 $\mathfrak{h}$. 如果在积 $\mathfrak{g}\mathfrak{h}$ 中羣子集之一，譬如說 $\mathfrak{g}$，是由一个元素 g 組成的，我們就把 $\mathfrak{g}\mathfrak{h}$ 簡写为 $g\mathfrak{h}$.

显然有下面的規律

$$\mathfrak{g}(\mathfrak{h}\mathfrak{k}) = (\mathfrak{g}\mathfrak{h})\mathfrak{k},$$

因此在羣子集的連乘积中，括号是可以去掉不用的［参看 §9，(1)］.

如果羣子集 $\mathfrak{g}$ 是一个子羣，那末就有

$$\mathfrak{g}\mathfrak{g} = \mathfrak{g}.$$

現在假設 $\mathfrak{g}$ 和 $\mathfrak{h}$ 是 $\mathfrak{G}$ 的子羣. 我們要問，在何种条件下积 $\mathfrak{g}\mathfrak{h}$ 仍是一个羣. $\mathfrak{g}\mathfrak{h}$ 中的元素的逆元素的全体即 $\mathfrak{h}\mathfrak{g}$，因为 gh 的逆元是 $h^{-1}g^{-1}$. 因此，要使得 $\mathfrak{g}\mathfrak{h}$ 仍是一个羣，就必須有

$$\mathfrak{h}\mathfrak{g} = \mathfrak{g}\mathfrak{h}, \tag{1}$$

即 $\mathfrak{g}$ 必須和 $\mathfrak{h}$ 可交換. 这个条件同时也是充分的. 如果这一条件成立，那么 $\mathfrak{g}\mathfrak{h}$ 在包含每一元素 gh 的同时也包含着它的逆元 $h^{-1}g^{-1}$；其次，由于

$$\mathfrak{g}\mathfrak{h}\mathfrak{g}\mathfrak{h} = \mathfrak{g}\mathfrak{g}\mathfrak{h}\mathfrak{h} = \mathfrak{g}\mathfrak{h},$$

$\mathfrak{g}\mathfrak{h}$ 在包含任意两个元素的同时也包含着它們的积. 因此，$\mathfrak{G}$ 的两个子羣 $\mathfrak{g}$ 和 $\mathfrak{h}$ 的积仍是一羣，当且仅当子羣 $\mathfrak{g}$ 和 $\mathfrak{h}$ 可交換. 这里

当然并不要求 $\mathfrak{g}$ 的每个元素和 $\mathfrak{h}$ 的每个元素可交换. 如果可交换性条件(1)成立,那末积 $\mathfrak{gh}$ 就是由 $\mathfrak{g}$ 和 $\mathfrak{h}$ 所生成的羣.

在一个 Abel 羣中,条件(1)是永远成立的. 当 Abel 羣是作为加羣給出时, $\mathfrak{g}$ 和 $\mathfrak{h}$ 就是一个模的子模, 我們把 $\mathfrak{gh}$ 写成 $(\mathfrak{g}, \mathfrak{h})$, 而記号 $\mathfrak{g}+\mathfrak{h}$ 則暫且保留下来, 用以表示下面将要討論的"直和"这一特殊情形.

如果 $\mathfrak{g}$ 是 $\mathfrak{G}$ 中的一个子羣, a 是 $\mathfrak{G}$ 里面的一个元素, 則羣子集 $a\mathfrak{g}$ 称为 $\mathfrak{g}$ 在 $\mathfrak{G}$ 中的一个左陪集, $\mathfrak{g}a$ 称为一个右陪集(也称为傍系,同余类等). 如果 a 在 $\mathfrak{g}$ 內,則 $a\mathfrak{g}=\mathfrak{g}$. 因此, $\mathfrak{g}$ 的左陪集(右陪集)当中总是有一个陪集和 $\mathfrak{g}$ 自身相同.

下面我們主要討論左陪集, 但所进行的一切討論也同样适用于右陪集.

两个陪集 $a\mathfrak{g}$, $b\mathfrak{g}$ 完全可以相等,而不必有 $a=b$. 事实上,只要 $a^{-1}b$ 属于 $\mathfrak{g}$ 就会有

$$b\mathfrak{g}=aa^{-1}b\mathfrak{g}=a(a^{-1}b\mathfrak{g})=a\mathfrak{g}.$$

两个不同的陪集不可能有公共的元素,因为如果陪集 $a\mathfrak{g}$ 和 $b\mathfrak{g}$ 有一个公共元素,譬如說,

$$ag_1=bg_2,$$

則必有

$$g_1g_2^{-1}=a^{-1}b,$$

因此 $a^{-1}b$ 属于 $\mathfrak{g}$; 根据以上所述, $a\mathfrak{g}$ 和 $b\mathfrak{g}$ 相等.

每一个元素 a 都属于某一个陪集,即陪集 $a\mathfrak{g}$. 根据以上所証, 元素 a 只能属于一个陪集. 这样,我們就可以把每个元素 a 看作是包含着 a 的陪集 $a\mathfrak{g}$ 的代表元素.

根据以上两小节所述, 陪集构成了羣 $\mathfrak{G}$ 的元素的一种分类.

每一个元素都属于一个类而且仅属于一个类[1]。

每两个陪集是等势的，因为通过 $ag \to bg$ 就可以定义 $a\mathfrak{g}$ 到 $b\mathfrak{g}$ 之上的一个 1-1 映射。

除了 $\mathfrak{g}$ 本身之外，其余的陪集都不是羣，因为一个羣必须包含着单位元素才行。

子羣 $\mathfrak{g}$ 在 $\mathfrak{G}$ 中的不同陪集的个数称为 $\mathfrak{g}$ 在 $\mathfrak{G}$ 中的指数。 指数可以是有限的，也可以是无限的。

設 N 是羣 $\mathfrak{G}$ 的阶数（假定它是有限的），n 是 $\mathfrak{g}$ 的阶数，j 是指数，则有关系式

$$N = jn \tag{2}$$

成立，因为 $\mathfrak{G}$ 可以分解成 j 个类，每个类包含 n 个元素[2]。

在有限羣的情形，可以由 (2) 来計算指数 j:

$$j = \frac{N}{n}.$$

推論. 有限羣的子羣的阶是整个羣的阶的因子。

特别，如果我們命所討論的子羣为由元素 c 所生成的循环羣，那末从这里可以推知：

在一个有限羣中，每个元素的阶数都是羣阶数的因子。

这一定理的一个直接的推論是：在一个具有 n 个元素的羣中，关系式 $a^n = e$ 对每个元素 a 成立。

可能出现这样的情况：即每一个左陪集 $a\mathfrak{g}$ 同时也是一个右陪

---

1) 在有些文献中經常可以看到由 Galois 所首先引入的記法：

$$\mathfrak{G} = a_1\mathfrak{g} + a_2\mathfrak{g} + \cdots,$$

这个記法的意义是說，陪集 $a_\nu\mathfrak{g}$ 彼此不相交，而它們的和等于整个羣 $\mathfrak{G}$。我們不采用这种記法，因为我們要把“+”这个記号保留下来，用来表示以后将要定义的直和。

2) 当 N 为无限时关系式也成立。但为了說明它的意义，必须引入基数的积的概念。这一点我們沒有作。

集. 在这一情况下,任意給定元素 a, 包含着 a 的那个左陪集必定和包含着 a 的那个右陪集相等,也就是說,对每个元素 a 都必有

$$ag = ga. \tag{3}$$

具有性質(3), 即和 $\mathfrak{G}$ 中每个元素 a 可交换的子羣 $\mathfrak{g}$ 称为 $\mathfrak{G}$ 的一个**正規子羣**或**不变子羣**.

如果 $\mathfrak{g}$ 是正規子羣,則两个陪集的积仍是陪集:

$$a\mathfrak{g}\cdot b\mathfrak{g} = a\cdot\mathfrak{g}b\cdot\mathfrak{g} = ab\mathfrak{g}\mathfrak{g} = ab\mathfrak{g}.$$

习題. 1. 試决定 $\mathfrak{S}_3$ 中各个子羣的左、右陪集, 这些子羣中哪一些是正規子羣?

2. 証明: 对任意子羣来說, 一个左陪集中的元素的逆元組成一个右陪集,并由此进一步断定,子羣的指数也可以定义为右陪集的个数.

3. 証明: 每一个指数为 2 的子羣是正規子羣. 例: n 个文字的对称羣中,交錯羣就是一个指数为 2 的子羣.

4. Abel 羣的子羣都是正規子羣.

5. 在一个羣中, 和每个元素都可交换的元素組成这羣中的一个正規子羣(羣的"**中心**").

6. 設 $\mathfrak{G}$ 是由 a 生成的一个循环羣, $\mathfrak{g}$ 是 $\mathfrak{G}$ 中一个不等于单位羣的子羣,它由具有最小正指数 m 的元素 a^m 生成(参看 § 10),則 $1, a, a^2, \cdots, a^{m-1}$ 是 $\mathfrak{g}$ 在 $\mathfrak{G}$ 中的全部陪集的代表元素,而 m 是 $\mathfrak{g}$ 在 $\mathfrak{G}$ 中的指数.

7. 如果 $\mathfrak{g}$ 在 $\mathfrak{G}$ 中的任意两个左陪集的积仍是一个左陪集, 則 $\mathfrak{g}$ 是 $\mathfrak{G}$ 中的正規子羣.

§ 12. 同构与自同构

現在假設給定了两个集合 $\mathfrak{M}$ 和 $\overline{\mathfrak{M}}$,并且在每个集合中都定义了元素之間的任意某种关系. 例如我們可以想象集合 $\mathfrak{M}$ 和 $\overline{\mathfrak{M}}$ 是两个羣,而元素之間的关系則是由于羣性質而成立的等式 $a\cdot b=c$; 也可想象这两个集合是有序的,而所考虑的关系是 $a > b$.

如果能够在这两个集合之間建立起一个 1-1 对应, 使得在这

一对应之下元素之間的关系保持不变，也就是說，如果 $\mathfrak{M}$ 中的每个元素 a 有 $\bar{\mathfrak{M}}$ 中的一个元素 $\bar{a}$ 与之双方单値地相对应，并且对 $\mathfrak{M}$ 中任意元素 $a, b, \cdots$ 成立的每一关系，对 $\bar{\mathfrak{M}}$ 中的相应元素 $\bar{a}, \bar{b}, \cdots$ 也成立，而反过来也是这样，我們就說，这两个集合（相对于所考慮的关系来說）是**同构的**，并且写 $\mathfrak{M} \simeq \bar{\mathfrak{M}}$. 而上述对应规則称为一个**同构**.

为了強調同构对应的双方单値性，我們也使用 1-**同构**的和 1-**同构**这样的說法.

这样一来，我們就可以討論**同构的羣**，同构的有序集或**相似有序**集等概念了. 两个羣之間的一个同构，就是这样一个 1-1 映射 $a \to \bar{a}$，在这个映射之下，由 $ab = c$ 即有 $\bar{a}\bar{b} = \bar{c}$（反之亦然），因而在这个映射之下与积 ab 相对应的是积 $\bar{a}\bar{b}$.

正好象在一般集合論中势相同的集合被看作是彼此等价一样，序型理論中的相似集，羣論中相互同构的羣也看作是本质上相同的对象. 在某一集合中的已給关系的基础之上所能建立起来的一切概念和定理，都可以直接地应用于每一个和它同构的集合. 举例来說，如果在一个集合中定义了乘积的关系，并且这个集合和一个羣同构，那末这个集合本身也是一个羣. 同构把单位元素、逆元素和子羣仍旧映成单位元素、逆元素和子羣.

特别，如果两个集合 $\mathfrak{M}$ 和 $\bar{\mathfrak{M}}$ 彼此重合，也就是說，如果所考慮的对应双方单値地把每个元素 a 映成同一集合中的元素 $\bar{a}$，并且保持元素之間的关系，这样一个对应就称为一个**自同构**（或 1-**自同构**）.

举例来說，当 $\mathfrak{M}$ 是整数的集合，而所考慮的基本关系是次序关系 $a < b$ 时，对应

$$a \to a + 1$$

就是一个自同构，因为这个对应把整数的集合双方单值地映射成其自身，并且由 $a<b$ 即有 $a+1<b+1$，反之亦然.

一个集合的自同构在一定的程度上表达了这个集合的对称性質. 事实上，一个几何图形的对称性究竟意味着什么呢？这就是說，它可以被某些变换（反射、旋轉等等）变成其自身，而在这些变换之下某些关系（如距离、角度、相对位置等）保持不变，用我們的語言来說，就是这个图形，就其度量性質来說，能够容許某些自同构.

两个自同构的积（即 § 9 中所講到的变换的积）显然仍是一个自同构，一个自同构的逆变换也是一个自同构. 因此，根据 § 9，一个任意集合（其元素之間定义了任意某些关系）的自同构組成一个变换羣：这个集合的自同构羣.

特别，一个羣的自同构本身又組成一个羣. 我們要对这些自同构当中的某一些作进一步的考察.

設 a 是一个固定的羣元素，那末把 x 变成

$$\bar{x}=axa^{-1} \tag{1}$$

的变换是一个自同构. 首先，由 (1) 可以唯一地解出 x 来：

$$x=a^{-1}\bar{x}a,$$

因此这个对应是双方单值的. 其次，我們有

$$\bar{x}\bar{y}=axa^{-1}\cdot aya^{-1}=a(xy)a^{-1}=\overline{xy},$$

所以这个对应是一个同构对应.

我們說 axa^{-1} 是由 x 經 a 变换得出的元素，并称元素 x 和 axa^{-1} 为共軛羣元素. 由元素 a 所决定的自同构 $x\rightarrow axa^{-1}$ 称为羣的內自同构. 所有其余的自同构（如果还有其余的自同构的話）称为外自同构.

在一个內自同构 $x\rightarrow axa^{-1}$ 的作用之下，子羣 $\mathfrak{g}$ 变成子羣

$a\mathfrak{g}a^{-1}$，这个子羣我們称之为和 $\mathfrak{g}$ 共軛的子羣.

如果子羣 $\mathfrak{g}$ 和它所有的共軛子羣相重合，即对每个元素 a 有

$$a\mathfrak{g}a^{-1} = \mathfrak{g}, \tag{2}$$

那末这就意味着子羣 $\mathfrak{g}$ 和每个元素 a 可交换：

$$a\mathfrak{g} = \mathfrak{g}a,$$

因而 $\mathfrak{g}$ 是一个正規子羣（§ 11）. 因此，我們知道：

在所有內自同构之下不变的子羣即是正規子羣.

这个定理說明了正規子羣的另一名称——不变子羣——的意义.

条件（2）也可以用一个較弱的条件

$$a\mathfrak{g}a^{-1} \subseteq \mathfrak{g} \tag{3}$$

来代替. 如果（3）对每个元素 a 成立，那末它对元素 a^{-1} 也成立，即

$$\begin{gathered} a^{-1}\mathfrak{g}a \subseteq \mathfrak{g}, \\ \mathfrak{g} \subseteq a\mathfrak{g}a^{-1}; \end{gathered} \tag{4}$$

由(3)和(4)即可得出(2)来. 因此

如果一个子羣在包含每一个元素 b 的同时也包含着所有的共軛元素 aba^{-1}，那末它就是一个正規子羣.

习題. 1. Abel 羣除单位变换之外沒有其它的內自同构. 試証由元素

$$e, a, b, c$$

組成，并具有运算法則

$$\begin{cases} a^2 = b^2 = c^2 = e, \\ ab = ba = c, \\ bc = cb = a, \\ ca = ac = b \end{cases}$$

的羣除单位变换之外沒有其它的內自同构，但有五个外自同构.

2. 在一个置换羣中，一个元素 b 的共軛元素 aba^{-1} 可以用下面的方法得出：先把 b 表成循环的乘积（§ 10），然后将置换 a 作用于这些循环中的数碼. 証明这样得到的置换确是 aba^{-1}，并利用这个定理来計算 aba^{-1}，其中

$$b = (12)(345),$$
$$a = (2345).$$

3. 試証对称羣 $\mathfrak{S}_3$ 沒有外自同构，但有六个內自同构。

4. 对称羣 $\mathfrak{S}_4$ 除了它本身及单位子羣之外只有以下两个正規子羣:

a) 交錯羣 $\mathfrak{A}_4$,

b) "Klein 四元羣" $\mathfrak{B}_4$, 它由置换

$$(1), \quad (12)(34), \quad (13)(24), \quad (14)(23)$$

組成。这是一个 Abel 羣，和問題 1 中抽象地定义的那个羣同构。

5. 如果 $\mathfrak{g}$ 是 $\mathfrak{G}$ 中的一个正規子羣，而 $\mathfrak{H}$ 是一个"中間子羣"

$$\mathfrak{g} \subseteq \mathfrak{H} \subseteq \mathfrak{G},$$

則 $\mathfrak{g}$ 也是 $\mathfrak{H}$ 中的正規子羣。

6. 所有的无限循环羣都和整数加羣同构。

7. 在一个羣 $\mathfrak{G}$ 中，和固定元素 a 可交換的元素 x，即滿足条件

$$xa = ax$$

的元素 x 組成一个羣，称为 a 的**正規化子**。a 的正規化子包含着 a 所生成的循环羣作为一个正規子羣。和 a 共軛的元素的个数等于它的正規化子在 $\mathfrak{G}$ 中的指数。

8. 羣 $\mathfrak{G}$ 中的元素可以分解成許多共軛元素类。当 $\mathfrak{G}$ 为有限羣时，每个类中元素的个数是 $\mathfrak{G}$ 的阶数的一个因子。单位元素和每个中心元素（§ 11，习題 5）单独构成一个类。

9. 設在一个阶为 p^n（p 为素数）的羣中，含有 p^λ 个元素的共軛类的数目是 a_λ，特別設 a_0 是中心元素的个数，則有关系式:

$$p^n = a_0 + a_1 p + a_2 p^2 + \cdots.$$

利用这一等式証明：一个 p^n 阶羣的中心除单位元素之外还包有其它元素。

§ 13. 同态。正規子羣。商羣

設在两个集合 $\mathfrak{M}$ 和 $\overline{\mathfrak{M}}$ 中給定了某些关系。如果 $\mathfrak{M}$ 中的每个元素 a 都有 $\overline{\mathfrak{M}}$ 中的一个元素 $\bar{a}$ 与之相对应，并且

1. $\overline{\mathfrak{M}}$ 中的每个元素 $\bar{a}$ 至少和 $\mathfrak{M}$ 中某一个元素相对应，

2. 对 $\mathfrak{M}$ 中的元素成立的每一关系对 $\overline{\mathfrak{M}}$ 中的相应元素也成立，

那末这样一个对应就称为一个同态. $\overline{\mathfrak{M}}$ 称为 $\mathfrak{M}$ 的一个同态象，或者說 $\overline{\mathfrak{M}}$ 同态于 $\mathfrak{M}$.

同态关系用記号 $\mathfrak{M} \sim \overline{\mathfrak{M}}$ 来表示. 如果 $\overline{\mathfrak{M}} \subseteq \mathfrak{M}$，也就是說，如果所考慮的同态是 $\mathfrak{M}$ 到它自身之內的一个映射，我們就称它为一个自同态.

如果所考慮的映射是双方单值的，并且同态性質在相反的方向也同样成立，那末这样一个同态就是前面已經講到过的同构.

集合 $\mathfrak{M}$ 中的那些元素，在同态映射之下被映成 $\overline{\mathfrak{M}}$ 中同一元素 $\bar{a}$ 者，可以归为一个类 $\mathfrak{a}$. 每个元素 a 都属于一个而且仅属于一个类 $\mathfrak{a}$. 这就是說，集合 $\mathfrak{M}$ 可以分解成为許多元素类，这些元素类和 $\overline{\mathfrak{M}}$ 中的元素双方单値地相对应.

例. 如果命单位元素和某一羣中的每个元素相对应，所得到的就是这个羣到单位羣的一个同态. 同样，如果命数 $+1$ 和偶置換相对应，命 -1 和奇置換相对应，就得到置換羣的一个同态，同态象是数 $+1$ 和 -1 的乘法羣.

如果将整数 m 映成某一羣中元素 a 的冪 a^m，那末这个映射就是整数加羣到元素 a 所生成的循环羣的一个同态. 事实上，在这个映射之下和 $m+n$ 的象将是积 $a^{m+n} = a^m a^n$. 如果 a 是一个无限阶元素，这个同态就是一个同构.

現在让我們专門研究羣的同态.

如果在集合 $\mathfrak{G}$ 中定义了元素的积 $\bar{a}\bar{b}$（即定义了 $\bar{a}\bar{b} = \bar{c}$ 这种形式的关系），并且有一个羣 $\mathfrak{G}$ 被同态地映射成 $\overline{\mathfrak{G}}$，那末 $\overline{\mathfrak{G}}$ 也是一个羣. 簡短地說，一个羣的同态象仍是一个羣.

証. 首先，$\overline{\mathfrak{G}}$ 中任意三个元素 $\bar{a}, \bar{b}, \bar{c}$ 必是 $\mathfrak{G}$ 中某三个元素，譬如說，a, b, c 的象. 由

$$ab \cdot c = a \cdot bc$$

立得

$$\overline{ab}\cdot\bar{c}=\bar{a}\cdot\overline{bc}.$$

其次，由

$$ae=a \qquad (对所有的 a)$$

可得

$$\bar{a}\bar{e}=\bar{a} \qquad (对所有的 \bar{a}),$$

而由

$$ba=e \qquad (b=a^{-1})$$

可得

$$\bar{b}\bar{a}=\bar{e}.$$

因此在 $\bar{\mathfrak{G}}$ 中有一个单位元素，并且每个元素 $\bar{a}$ 都有一个逆元素。这就是說，$\bar{\mathfrak{G}}$ 是一个羣。与此同时我們还証明了下面的結論：

同态映射把单位元素变为单位元素，逆元素变为逆元素。

現在让我們对同态映射 $\mathfrak{G}\sim\bar{\mathfrak{G}}$ 所决定的分类作更深入一步的考察。在这里我們要建立起同态和正規子羣之間的一个重要关系。

羣 $\mathfrak{G}$ 中被同态 $\mathfrak{G}\sim\bar{\mathfrak{G}}$ 映射成 $\bar{\mathfrak{G}}$ 中单位元素 $\bar{e}$ 的元素类 $\mathfrak{e}$ 是 $\mathfrak{G}$ 的一个正規子羣，其余的元素类是这个正規子羣的陪集。

証。 首先可証 $\mathfrak{e}$ 是一个子羣。如果 a 和 b 被这个同态映射成 $\bar{e}$，則 ab 将被映射成 $\bar{e}^2=\bar{e}$；因此 $\mathfrak{e}$ 在包含任意两个元素的同时也包含着它們的积。其次，a^{-1} 被映射成 $\bar{e}^{-1}=\bar{e}$，因此 $\mathfrak{e}$ 也包含着每一个元素的逆元素。

左陪集 $a\mathfrak{e}$ 中的元素全都被映射成元素 $\bar{a}\bar{e}=\bar{a}$。反之，如果 a' 被映射成 $\bar{a}$，那末可以找到一个元素 x，使得

$$ax=a'.$$

这时将有

$$\bar{a}\bar{x} = \bar{a},$$

即

$$\bar{x} = \bar{e}.$$

这就是說，x 属于 $\mathfrak{e}$，因而 a' 属于 $a\mathfrak{e}$.

这样，羣 $\mathfrak{G}$ 中被映射成元素 $\bar{a}$ 的元素类恰好就是左陪集 $a\mathfrak{e}$.

完全同样地可以証明，被映射成 $\bar{a}$ 的元素类同时也必定是右陪集 $\mathfrak{e}a$. 因此，左陪集和右陪集相重合

$$a\mathfrak{e} = \mathfrak{e}a,$$

即 $\mathfrak{e}$ 是一个正規子羣. 这就完成了我們的証明.

正規子羣 $\mathfrak{e}$ 中的元素在所給的同态之下被映射成单位元素 $\bar{e}$，这个正規子羣称为所給同态的核.

现在让我們提出一个相反的問題：假設已經給定了 $\mathfrak{G}$ 的一个正規子羣 $\mathfrak{g}$，能不能造出一个同态于 $\mathfrak{G}$ 的羣 $\bar{\mathfrak{G}}$ 来，使得 $\mathfrak{g}$ 的陪集恰好和 $\bar{\mathfrak{G}}$ 的元素相对应？

为了达到这个目的，我們直接取 $\mathfrak{g}$ 的陪集本身作为所要造出的羣 $\bar{\mathfrak{G}}$ 的元素. 根据 § 11，正規子羣 $\mathfrak{g}$ 的两个陪集的积仍是一个陪集，并且如果 a 属于陪集 $a\mathfrak{g}$，b 属于陪集 $b\mathfrak{g}$，則 ab 属于陪集 $a\mathfrak{g}\cdot b\mathfrak{g} = ab\mathfrak{g}$. 因此，$\mathfrak{g}$ 的陪集組成一个同态于 $\mathfrak{G}$ 的集合，因而是一个同态于 $\mathfrak{G}$ 的羣. 我們称这个羣为 $\mathfrak{G}$ 对 $\mathfrak{g}$ 的商羣，并用記号

$$\mathfrak{G}/\mathfrak{g}$$

来表示它. $\mathfrak{G}/\mathfrak{g}$ 的阶就是 $\mathfrak{g}$ 的指数.

这里我們可以看到正規子羣的基本重要意义：它使得我們能够造出同态于已給羣的新羣来.

我們看到，如果一个羣 $\mathfrak{G}$ 被同态地映射成另一羣 $\bar{\mathfrak{G}}$，那末 $\bar{\mathfrak{G}}$ 的元素和同态核 $\mathfrak{e}$ 在 $\mathfrak{G}$ 中的陪集（双方单値地）相对应. 这一对应显然是一个同构. 事实上，如果 $a\mathfrak{g}$ 和 $b\mathfrak{g}$ 是两个陪集，則它們的积

将是 $ab\mathfrak{g}$；这三个陪集在 $\bar{\mathfrak{G}}$ 中的相应元素将是 $\bar{a}$, $\bar{b}$ 和 $\overline{(ab)}$，而由同态性质可知

$$\overline{(ab)} = \bar{a}\cdot\bar{b}.$$

这样一来，我們就得出了

$$\mathfrak{G}/\mathfrak{e} \simeq \bar{\mathfrak{G}}.$$

这样，我們就証明了羣的同态定理：

如果羣 $\mathfrak{G}$ 被同态地映射成羣 $\bar{\mathfrak{G}}$，則 $\bar{\mathfrak{G}}$ 和商羣 $\mathfrak{G}/\mathfrak{e}$ 同构；其中 $\mathfrak{e}$ 是同态的核。反之，羣 $\mathfrak{G}$ 可同态地映射成每个商羣 $\mathfrak{G}/\mathfrak{e}$（其中 $\mathfrak{e}$ 为正規子羣）。

习題. 1. 每个羣 $\mathfrak{G}$ 有两个显而易見的商羣：$\mathfrak{G}/\mathfrak{E} \simeq \mathfrak{G}$；$\mathfrak{G}/\mathfrak{G} \simeq \mathfrak{E}$.

2. 交錯羣的商羣 $(\mathfrak{S}_n/\mathfrak{A}_n)$ 是一个 2 阶循环羣.

3. Klein 四元羣（§ 12 习題 4）的商羣 $\mathfrak{S}_4/\mathfrak{B}_4$ 和 $\mathfrak{S}_3$ 同构.

4. 羣 $\mathfrak{G}$ 中形如 $aba^{-1}b^{-1}$ 的元素及此种元素的积組成一个羣，称为 $\mathfrak{G}$ 的换位子羣. 换位子羣是正規子羣，它的商羣是 Abel 羣. 如果一个正規子羣的商羣是 Abel 羣，这个正規子羣必定包含换位子羣.

5. 和一个子羣 $\mathfrak{g}$ 可交換的元素組成一个以 $\mathfrak{g}$ 为正規子羣的羣 $\mathfrak{h}$. $\mathfrak{h}$ 称为 $\mathfrak{g}$ 的正規化子. $\mathfrak{h}$ 在 $\mathfrak{G}$ 中的指数即 $\mathfrak{G}$ 中和 $\mathfrak{g}$ 共軛的子羣的个数.

6. 如果 $\mathfrak{G}$ 是一个循环羣，a 是它的生成元，$\mathfrak{g}$ 是一个指数为 m 的子羣，則 $\mathfrak{G}/\mathfrak{g}$ 是一个 m 阶循环羣. 元素 $1, a, a^2, \cdots, a^{m-1}$ 可取为 $\mathfrak{g}$ 的陪集的代表元素.

在一个 Abel 羣中，每一个子羣都是正規子羣（参看 § 11，习題 4）. 前面已經講过，如果把羣运算記成加法，那末 Abel 羣及其子羣称为模. 陪集 $a+\mathfrak{M}$ 称为 $\mathfrak{G}$ 对 $\mathfrak{M}$ 的同余类，而商羣 $\mathfrak{G}/\mathfrak{M}$ 則称为 $\mathfrak{G}$ 对 $\mathfrak{M}$ 的同余类模.

两个元素 a, b 属于同一同余类，当且仅当它們的差属于 $\mathfrak{M}$. 这样两个元素称为对 $\mathfrak{M}$ 同余，我們写

$$a \equiv b \pmod{\mathfrak{M}},$$

或簡写作

$$a \equiv b(\mathfrak{M}).$$

如果 a 和 b（对 $\mathfrak{M}$）同余，则在同态 $\mathfrak{G} \sim \mathfrak{G}/\mathfrak{M}$ 下同余类模中的相应元素 $\bar{a}$, $\bar{b}$ 相等；反之，如果 $\bar{a} = \bar{b}$，则 $a \equiv b(\mathrm{mod}\ \mathfrak{M})$.

举例来説，在整数系統中一个数 m 的所有倍数显然組成一个模。因此，如果差 $a-b$ 可被 m 整除，我們就写

$$a \equiv b(m).$$

在这一情况下同余类可由 $0, 1, 2, \cdots, m-1$ 来代表，而同余类模则是一个 m 阶循环羣。

习题.　7. 每个 m 阶循环羣都和整数加羣对整数 m 的同余类羣同构。

第三章　环与域

內容.　环、整环、域的定义. 由环来构造其它的环(以及域)的一般方法. 整环中的素因子分解定理.

本章的概念在全书中都要用到.

§14.　环

代数与算术中的运算对象是各种各样的:有时是整数,有时是有理数、实数、复数、代数数;还有 n 个变元的多項式或者有理函数等等. 以后我們还会有完全不同性質的对象: 超复数、同余类等等. 因此有必要以一个共同的概念把这些对象概括起来,并且一般地来研究这些系統中的运算規律.

所謂具有两个运算的系統就是指元素 $a, b, \cdots$ 的一个集合,其中每两个元素 a, b 都唯一地决定一个和 $a+b$ 以及一个积 $a\cdot b$,它們还属于这个集合.

一具有两个运算的系統称为环,如果对于系統中所有的元素,以下的运算規律成立:

I. 加法的規律.

a) 結合律: $a+(b+c)=(a+b)+c$.

b) 交換律: $a+b=b+a$.

c) 方程 $a+x=b$ 的可解性[1],对所有的 a 与 b.

---

1) 解的唯一性不必要求,以后可以推出.

II. 乘法的規律.

a) 結合律: $a\cdot bc = ab\cdot c$.

III. 分配律.

a) $a\cdot(b+c) = ab + ac$.

b) $(b+c)\cdot a = ba + ca$.

附注. 如果乘法还适合交换律:

II. b) $a\cdot b = b\cdot a$,

那么这个环就称为交換的,以前我們碰到的主要是交换环.

关于加法的規律. 三条規律 Ia, b, c 合起来正是說明了环元素对于加法組成一 Abel 羣[1]. 因此以前对于 Abel 羣証明了的定理全可以搬到环上来:存在一个(且只有一个)零元素 0 具有性质

$$a + 0 = a \quad \text{对所有的 } a.$$

对于每个元素 a 还有一个負元素 $-a$ 具有性质

$$-a + a = 0.$$

方程 $a + x = b$ 不但是可解的,并且解是唯一的;它的唯一的解是

$$x = -a + b;$$

我們記之为 $b - a$. 因为每个差根据

$$a - b = a + (-b)$$

都能改写成和,所以在这个意义上,差与和一样,次序可以改变,譬如

$$(a - b) - c = (a - c) - b,$$

等等. 最后, $-(-a) = a$ 与 $a - a = 0$.

关于結合律. 正如我們在第二章 § 9 中看到的,根据乘法的結合律我們可以定义連乘积

1) 这个羣称为环的加法羣.

$$\prod_{1}^{n} a_\nu = a_1 a_2 \cdots a_n,$$

并且有主要性质

$$\prod_{1}^{m} a_\mu \cdot \prod_{\nu=1}^{n} a_{m+\nu} = \prod_{1}^{m+n} a_\nu.$$

同样可以定义連加和

$$\sum_{1}^{n} a_\nu = a_1 + a_2 + \cdots + a_n,$$

并且証明它的主要性質

$$\sum_{1}^{m} a_\mu + \sum_{\nu=1}^{n} a_{m+\nu} = \sum_{1}^{m+n} a_\nu.$$

利用Ib,連加和中項的次序可以任意改变,在交換环中連乘积也有同样的性質.

关于分配律. 当乘法适合交換律时, IIIb 自然就是 IIIa 的推論.

对 n 作完全归納法由 IIIa 立即推出

$$a(b_1 + b_2 + \cdots + b_n) = ab_1 + ab_2 + \cdots + ab_n.$$

同样由 IIIb 推出

$$(a_1 + a_2 + \cdots + a_n)b = a_1 b + a_2 b + \cdots + a_n b.$$

把二者合起来就有通常和的乘积的規律:

$$\begin{aligned}
(a_1 + \cdots + a_n)(b_1 + \cdots + b_m) \\
&= a_1 b_1 + \cdots + a_1 b_m \\
&\quad + \cdots\cdots \\
&\quad + a_n b_1 + \cdots + a_n b_m \\
&= \sum_{i=1}^{n} \sum_{k=1}^{m} a_i b_k.
\end{aligned}$$

減法也适合分配律,譬如

$$a(b - c) = ab - ac,$$

这个由

$$a(b-c)+ac=a(b-c+c)=ab$$

即得.

特别地是

$$a\cdot 0=a(a-a)=a\cdot a-a\cdot a=0,$$

这就是：当一个因子是零时，乘积一定等于零.

在下面的例子中将看到，这个定理的逆不一定成立：可能有

$$a\cdot b=0,\quad a\neq 0,\quad b\neq 0.$$

在这个情形，我們称 a 与 b 为零因子，确切地説，a 是左零因子，b 是右零因子.（在交换环中这两个概念沒有区别.）把零本身也看成是零因子是方便的. 因此，a 称为左零因子，如果有一 $b\neq 0$ 使 $ab=0$[1].

如果在一环中除去零以外不再有零因子，也就是說，由 $ab=0$ 必然推出 $a=0$ 或者 $b=0$，那么这个环就称为无零因子的环. 如果这个环又是交换的，那么它就称为整环.

例. 所有开始时提到的例子（整数环、有理数等）都是无零因子的环. 区間 $(-1,+1)$ 上連續函数的环有零因子，因为对于

$$f=f(x)=\max(0,x),$$

$$g=g(x)=\max(0,-x),$$

就有 $f\neq 0$[2]，$g\neq 0$，$fg=0$.

习题. 1. 整数偶 (a_1,a_2) 对于运算

$$(a_1,a_2)+(b_1,b_2)=(a_1+b_1,a_2+b_2),$$

$$(a_1,a_2)\cdot(b_1,b_2)=(a_1b_1,a_2b_2)$$

---

1) 假定在环中有 $\neq 0$ 的元素.

2) $f\neq 0$ 表示：f 不是零函数. 这并不是說 f 完全不取零作为函数值.

組成一有零因子的环。

2. 如果 a 不是左零因子，那么方程 $ax = ay$ 中 a 可以消去。（特别在整环中任意的 $a \neq 0$ 都可以消去。）

3. 我們可以造一个环，以任意的交换羣作为它的加法羣，其中任意两个元素的乘积全等于零。

单位元素. 如果一个环有一个左单位元素 e:

$$ex = x \quad \text{对所有的 } x$$

并且同时又有一个右单位元素 e':

$$xe' = x \quad \text{对所有的 } x,$$

那么它們必須相等，因为

$$e = ee' = e'.$$

于是每一个右单位元素和左单位元素都等于 e. 我們簡单地就称 e 为单位元素并且說这是一个具有单位元素的环. 单位元素常常就用 1 表示，虽然它与数 1 是需要区别开的.

整数組成一具有单位元素的环，偶数組成的环沒有单位元素. 存在这样的环，它有一个或者許多个右单位元素，但是沒有左单位元素，或者反过来.

逆元素. 設 a 是一具有单位元素 e 的环中任意一个元素，所謂 a 的一个左逆是指这样一个元素 $a_{(l)}^{-1}$:

$$a_{(l)}^{-1}a = e,$$

一个右逆是指元素 $a_{(r)}^{-1}$:

$$aa_{(r)}^{-1} = e.$$

如果元素 a 既有左逆又有右逆，那么它們一定相等，因为

$$a_{(l)}^{-1} = a_{(l)}^{-1}(aa_{(r)}^{-1}) = (a_{(l)}^{-1}a)a_{(r)}^{-1} = a_{(r)}^{-1},$$

因此 a 的每个左逆与右逆全相等. 在这个情形我們就說：a 有逆元素，这个逆元素記为 a^{-1}.

冪与倍. 在第二章中已經看到，根据結合律，对于每一个环

元素 a 我們可以定义幂 a^n (n 是自然数)，它适合通常的規則：

$$(1)\qquad \begin{cases} a^n \cdot a^m = a^{n+m}, \\ (a^n)^m = a^{nm}, \\ (ab)^n = a^n b^n. \end{cases}$$

最后一条只对交換环成立。

如果这个环有单位元素并且 a 有逆，我們还可以引入次数为零或負数的幂 (§ 9)；規則 (1) 仍然成立。

同样在环的加法羣中可以定义倍元

$$n \cdot a \quad (= a + a + \cdots + a \quad n \text{ 項})$$

并且有

$$(2)\qquad \begin{cases} na + ma = (n+m)a, \\ n \cdot ma = nm \cdot a, \\ n(a+b) = na + nb, \\ n \cdot ab = na \cdot b = a \cdot nb. \end{cases}$$

象对于幂一样，令

$$(-n) \cdot a = -na,$$

于是規則 (2) 对于所有的整数 n 与 m (正、負和零)都成立。

应該注意，不能把 $n \cdot a$ 了解为两个环元素的乘积；因为一般地 n 不是环中的元素，而是由外边引入的一个整数。 如果这个环有单位元素，那么 na 可以写成眞正的乘积，即

$$na = n \cdot ea = ne \cdot a.$$

习題． 4．証明，左零因子沒有左逆，右零因子沒有右逆．特别零元素既沒有左逆又沒有右逆． 一个平凡的例外：在由单个的元素 0 組成的环中，2同时就是单位元素，也就是逆元素("零环")．

5．对于任意的交换环，对 n 作完全归納法証明二項式定理：

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \cdots + b^n,$$

这里$\binom{n}{k}$表示整数

$$\frac{n(n-1)\cdots(n-k+1)}{1\cdot 2\cdots k}=\frac{n!}{(n-k)!k!}.$$

6. 証明,在恰有 n 个元素的环中,对每个 a 有

$$n\cdot a=0.$$

[参看 § 11, 那里証明了 $a^n=e$.]

7. 如果 a 与 b 可交换,即 $ab=ba$, 那么 a 与 $-b$,与 nb, 与 b^{-1} 也可交换. 如果 a 与 b, c 可交换,那么 a 与 $b+c$, bc 也可交换.

域. 一个环称为体,如果

a) 它至少有一个非零元素,

b) 方程

$$\begin{cases}ax=b,\\ ya=b.\end{cases}\tag{3}$$

对任意 $a\neq 0$ 可解.

如果这个环又是交换的,那么它就称为域[1].

正如对于羣一样(第二章),由 a) 与 b) 可証明:

c) 存在一个左单位元素 e. 对于任意的 $a\neq 0$, 解方程 $xa=a$, 記解为 e. 如果 b 是任意元素,那么解方程 $ax=b$;由此推出

$$eb=eax=ax=b.$$

同样,存在一个右单位元素,因之,存在单位元素.

由 c) 立即推出:

d) 对每个 $a\neq 0$, 存在一左逆,同样存在一右逆, 因之, 存在逆元素.

正如在羣中所証明的,由 c) 与 d) 反过来可以推出 b).

1) 有些作者把体称为域,然后分成交换的与非交换的域.

习题. 8. 作出以上的証明.

体沒有零因子，因为由 $ab=0$，$a\neq 0$，两边乘以 a^{-1} 立即推出 $b=0$.

方程(3)的解是唯一的；假如第一个方程有两个解 x，x'，于是

$$ax=ax',$$

从左边乘上 a^{-1} 即得

$$x=x'.$$

(3) 的解就是

$$x=a^{-1}b,$$

$$y=ba^{-1}.$$

在交换的情形有 $a^{-1}b=ba^{-1}$，我們就写成 $\frac{b}{a}$.

体中非零元素对于乘法組成一个羣：体的乘法羣.

因之体是两个羣的联合：一个乘法羣和一个加法羣. 这两个羣通过分配律联系起来.

例. 1. 有理数、实数、复数都組成域.

2. 我們按以下的办法构造一个只由 0，1 两个元素組成的域：乘法就按通常 0，1 这两个数的乘法. 对于加法，0 是零元素：

$$0+0=0,\quad 0+1=1+0=1;$$

再令 $1+1=0$. 这个加法正如两个元素的循环羣中的运算一样(§10)，因此适合加法的規律. 乘法的規律成立，因为它們对于普通的数 0，1 是成立的. 至于第一个分配律，我們列举所有的可能性来加以証明：当其中出現一个零，結論是显然的；因之剩下只要驗証

$$1\cdot(1+1)=1\cdot 1+1\cdot 1,$$

这个归結为 $0=0$. 最后，方程 $1\cdot x=a$ 对每个 a 都有解，解就是 $x=a$.

习题. 9. 构造一个三个元素的域. [首先討論,它的加法与乘法羣可能有怎样的結构.]

10. 有限多个元素的整环是域. [参看第二章§9中相应的羣論定理.]

§15. 同态与同构

設 $\mathfrak{S}$, $\bar{\mathfrak{S}}$ 是具有两个运算的系統,有一个 $\mathfrak{S}$ 到 $\bar{\mathfrak{S}}$ 上的映射,这就是說, $\mathfrak{S}$ 中每个 a 都有 $\bar{\mathfrak{S}}$ 中一个元素 $\bar{a}$ 与之对应并且对于 $\bar{\mathfrak{S}}$ 中每个 $\bar{a}$ 都至少有 $\mathfrak{S}$ 中一个元素对应过来, 这个映射称为**同态映射**(有时簡称同态),如果由 $a \to \bar{a}$ 与 $b \to \bar{b}$ 必有

$$a + b \to \bar{a} + \bar{b}$$

与

$$a \cdot b \to \bar{a} \cdot \bar{b},$$

$\bar{\mathfrak{S}}$ 就称为 $\mathfrak{S}$ 的一个**同态象**. 記为 $\mathfrak{S} \sim \bar{\mathfrak{S}}$.

如果这个映射又是 1-1 的,这就是說,与每个 $\bar{a}$ 对应的恰有一个元素 a ,那么它就称为**同构映射**(有时簡称同构). 記为 $\mathfrak{S} \simeq \bar{\mathfrak{S}}$. 系統 $\mathfrak{S}$ 与 $\bar{\mathfrak{S}}$ 就称为**同构的**. 关系 $\mathfrak{S} \simeq \bar{\mathfrak{S}}$ 是自反的、传递的并且因为同构映射的逆映射也是同构映射,所以是对称的.

环的同态象也是环.

証明. 設 $\mathfrak{R}$ 是一环, $\bar{\mathfrak{R}}$ 是一具有两个运算的系統, 并且 $\mathfrak{R} \sim \bar{\mathfrak{R}}$. 我們要来証明 $\bar{\mathfrak{R}}$ 也是环. 証明的步驟与羣的情形(§13)一样:

設 $\bar{a}$, $\bar{b}$, $\bar{c}$ 是 $\bar{\mathfrak{R}}$ 中任意三个元素. 为了証明各条运算規律,譬如 $\bar{a}(\bar{b}+\bar{c}) = \bar{a}\bar{b} + \bar{a}\bar{c}$,任取 $\bar{a}$, $\bar{b}$, $\bar{c}$ 的三个原象 a, b, c. 因为 $\mathfrak{R}$ 是环,所以 $a(b+c) = ab + ac$,根据同态映射的定义推知 $\bar{a}(\bar{b}+\bar{c}) = \bar{a}\bar{b} + \bar{a}\bar{c}$. 所有的結合,交換和分配律可以同样証明. 为了証明方程 $\bar{a} + \bar{x} = \bar{b}$ 的可解性, 任取 $\bar{a}$, $\bar{b}$ 的原象 a, b, 解方程 $a + x = b$,經过同态映射即得 $\bar{a} + \bar{x} = \bar{b}$.

在同态映射下，$\mathfrak{R}$ 的零元素 0 与任意元素 a 的負元素映到 $\bar{\mathfrak{R}}$ 中的零元素与負元素．如果 $\mathfrak{R}$ 有单位元素 e，那么它也映到 $\bar{\mathfrak{R}}$ 的单位元素．

証明与羣的情形一样．

如果 $\mathfrak{R}$ 是交換的，显然 $\bar{\mathfrak{R}}$ 也是．

当 $\mathfrak{R}$ 是一整环，下面我們将看到，$\bar{\mathfrak{R}}$ 不一定是整环；当 $\mathfrak{R}$ 不是整环时，$\bar{\mathfrak{R}}$ 有可能是整环．如果映射是同构的，那么 $\bar{\mathfrak{R}}$ 具有 $\mathfrak{R}$ 的全部代数性质．由此推出

整环与域的同构象分别是整环与域．

下面的定理在这里看起来几乎是沒有什么意义的，但是以后我們会看到它的重要作用：

設 $\mathfrak{R}$ 与 $\mathfrak{S}'$ 是两个沒有公共元素的环．$\mathfrak{S}'$ 包含一个子环 $\mathfrak{R}'$ 与 $\mathfrak{R}$ 同构．于是存在一个环 $\mathfrak{S} \simeq \mathfrak{S}'$．$\mathfrak{S}$ 包含 $\mathfrak{R}$ 作为子环．

証明． 我們从 $\mathfrak{S}'$ 中挖出 $\mathfrak{R}'$ 的元素并且用 $\mathfrak{R}$ 中在同构映射下与它們对应的元素来代替．对于原来的元素与替进来的元素我們如此定义和与积，使它們恰与 $\mathfrak{S}'$ 中的和与积对应．（例如，在代替前为 $a'b' = c'$，a' 被 a 代替，而 b' 与 c' 經过代替沒有变，那么就定义：$ab' = c'$．）这样，我們就得到一个环 $\mathfrak{S} \simeq \mathfrak{S}'$，$\mathfrak{S}$ 确实包含 $\mathfrak{R}$．

§16. 商的构成

如果交換环 $\mathfrak{R}$ 是嵌在一个体 Ω 中，那么在 Ω 中由 $\mathfrak{R}$ 的元素可以作商

$$\frac{a}{b} = ab^{-1} = b^{-1}a \quad (b \neq 0)^{1)}.$$

---

1) 由 $ab = ba$ 推出 $ab^{-1} = b^{-1}a$，这只要从左边和右边都乘上 b^{-1} 即得．

对于商，下面的运算规律成立：

$$(1)\qquad \begin{cases} \dfrac{a}{b}=\dfrac{c}{d} \quad \text{当且仅当 } ad=bc; \\ \dfrac{a}{b}+\dfrac{c}{d}=\dfrac{ad+bc}{bd}; \\ \dfrac{a}{b}\cdot\dfrac{c}{d}=\dfrac{ac}{bd}. \end{cases}$$

在上面这些式子的两边都乘以 bd 我們就得到等式，再由 $bdx=bdy$ 推出 $x=y$，这就証明了以上的規律.

因此我們看到，商 a/b 組成一域 $\mathbf{P}$，它称为交换环 $\mathfrak{R}$ 的**商域**. 由規律 (1) 我們还看到，只要能对分子与分母，也就是 $\mathfrak{R}$ 中的元素进行运算，那么分式的相等，相加与相乘的方法也就知道了，换句話說，商域 $\mathbf{P}$ 的結构完全被 $\mathfrak{R}$ 的結构决定，也就是：**同构的环的商域也同构**. 特别，一个环的两个商域一定是同构的，也就是：**如果环 $\mathfrak{R}$ 有商域，那么商域 $\mathbf{P}$ 在同构之下是被环 $\mathfrak{R}$ 唯一决定**.

我們現在問：什么样的环有一个商域？或者换个說法，什么样的环可以嵌入一个域？

如果环 $\mathfrak{R}$ 可以嵌入一个域，那么首先要求在 $\mathfrak{R}$ 中沒有零因子；因为域是沒有零因子的. 在交换的情形，这个条件也是充分的：**每一个整环都能够嵌入一个域**[1].

証明. 我們可以把 $\mathfrak{R}$ 只由单个的零元素組成这个平凡的情形除外. 我們考虑所有元素偶 (a, b)，$b\neq 0$ 的集合. 这样的元素偶下面将与商 a/b 对应.

我們規定 $(a, b)\sim(c, d)$，当 $ad=bc$. [参看前面的公式 (1).] 这样定义的关系显然是自反的和对称的；它也是传递的，因

1) 对于非交换的无零因子的环这个定理不再成立；参看 A. Malcev: *Math. Ann.*, **113** (1936).

为由

$$(a, b) \sim (c, d), \quad (c, d) \sim (e, f)$$

推出

$$ad = bc, \quad cf = de,$$

从而

$$adf = bcf = bde,$$

根据 $d \neq 0$ 以及 $\mathfrak{R}$ 的交换性即得：

$$af = be,$$

$$(a, b) \sim (e, f).$$

因之，关系 $\sim$ 具有等价关系的全部性质；根据第一章 §5 它就对于元素偶 (a, b) 定义一个分类，等价的元素偶属于同一类。元素偶 (a, b) 所在的一类用符号 a/b 表示。根据这个定义，$a/b = c/d$ 当且仅当 $(a, b) \sim (c, d)$，也就是 $ad = bc$。

相应于前面的公式 (1) 我們**定义**这些新符号 a/b 的和与积如下：

(2) $$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

(3) $$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

这个定义是合理的；因为首先，当 $b \neq 0$ 与 $d \neq 0$ 时有 $bd \neq 0$，所以 $\frac{ad + bc}{bd}$ 与 $\frac{ac}{bd}$ 是可以允許的符号；其次，右端的結果是与类 $\frac{a}{b}$ 与 $\frac{c}{d}$ 中代表 (a, b) 与 (c, d) 的选择无关。在 (2) 中把 a 与 b 换成 a' 与 b'，这里

$$ab' = a'b,$$

于是推出

$$adb' = a'db,$$

$$adb' + bcb' = a'db + b'cb,$$
$$(ad + bc)b'd = (a'd + b'c)bd,$$

从而

$$\frac{ad + bc}{bd} = \frac{a'd + b'c}{b'd}.$$

同样地

$$ab' = ba',$$
$$acb'd = a'cbd,$$
$$\frac{ac}{bd} = \frac{a'c}{b'd}.$$

把 (c, d) 换成 (c', d') 也有相应的結果，这里 $cd' = c'd$.

不难証明，全部域的性质是满足的. 例如，加法的結合律就是：

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf + de}{df} = \frac{adf + bcf + bde}{bdf},$$
$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{adf + bcf + bde}{bdf},$$

其余規律的証明类似.

这个构造出来的域显然是交換的. 为了証明它包含环 $\mathfrak{R}$，我們必須把某些商与 $\mathfrak{R}$ 的元素等同起来. 作法如下：

让所有的商 $\frac{cb}{b}$ 与元素 c 对应，其中 $b \neq 0$. 这些商都相等：

$$\frac{cb}{b} = \frac{cb'}{b'}, \quad \text{因为} (cb)b' = b(cb').$$

因之每个元素 c 只与一个商对应. 不同的元素 c, c' 对应的商也不同；因为由

$$\frac{cb}{b} = \frac{c'b'}{b'}$$

推出

$$cbb' = bc'b',$$

由于 $b \neq 0$, $b' \neq 0$, 所以它們可以消去:

$$c = c'.$$

因此 $\Re$ 的元素 1-1 地对应到某些商。

如果在 $\Re$ 中 $c_1 + c_2 = c_3$ 或者 $c_1c_2 = c_3$, 那么对于任意的 $b_1 \neq 0$, $b_2 \neq 0$ 以及 $b_3 = b_1b_2$ 有

$$\frac{c_1b_1}{b_1} + \frac{c_2b_2}{b_2} = \frac{c_1b_1b_2 + c_2b_1b_2}{b_1b_2} = \frac{c_3b_3}{b_3},$$

或者

$$\frac{c_1b_1}{b_1} \cdot \frac{c_2b_2}{b_2} = \frac{c_1c_2b_1b_2}{b_1b_2} = \frac{c_3b_3}{b_3}.$$

对应的商 $\frac{c_ib_i}{b_i}$ 相加与相乘正好与环元素 c_i 是一致的; 它們組成一个与 $\Re$ 同构的环. 因此我們可以把商 $\frac{cb}{b}$ 換成对应的元素 c (§ 15 最后). 这样就証明了,这个域包含环 $\Re$.

于是我們証明了对于每个整环 $\Re$ 都存在一个包含它的域.

构造商域是由一个环造出另一个环(有时是域)的第一个方法. 例如,按这个方法由通常的整数环 C 就得出了有理数域 Γ.

习題. 証明:每个交換环 $\Re$ (有或者沒有零因子) 都可以嵌入一个"商环",它是由所有的商 a/b (b 取遍所有的非零因子) 組成. 一般地,設 $\mathfrak{M}$ 是非零因子的一个集合,它具有性質: 如果 b_1, b_2 属于 $\mathfrak{M}$, 则 b_1b_2 也属于 $\mathfrak{M}$, 于是商 a/b, 其中 b 是 $\mathfrak{M}$ 中任意元素, 也組成一个商环 $\Re_{\mathfrak{M}}$.

§ 17. 向量空間与代数

設 $\Re$ 是一个具有单位元素的环, 它的元素用希腊字母 α, β, $\cdots$ 表示, $\mathfrak{G}$ 是一个加法 Abel 羣, 它的元素为 u, v, $\cdots$.

模 $\mathfrak{G}$ 称为 $\Re$ 上的一个 n **元綫性齐式模**或者一个 n **維向量空間**, 如果除去 $\mathfrak{G}$ 中的加法外还定义了 $\mathfrak{G}$ 中元素与 $\Re$ 中元素的乘

积，它具有以下的性质：

1. $\mathfrak{R}$ 中元素 α 与 $\mathfrak{G}$ 中元素 u 的乘积 αu 属于 $\mathfrak{G}$.

2. $\alpha(u+v)=\alpha u+\alpha v$.

3. $(\alpha+\beta)u=\alpha u+\beta u$.

4. $(\alpha\beta)u=\alpha(\beta u)$.

5. $\mathfrak{G}$ 中所有的元素都能唯一地表示成 n 个固定的"基元素" $u_1,\cdots,u_n$ 的綫性齐式 $\alpha_1 u_1+\cdots+\alpha_n u_n$.

由 2. 与 4. 推出

$$\beta(\alpha_1 u_1+\cdots+\alpha_n u_n)=(\beta\alpha_1)u_1+\cdots+(\beta\alpha_n)u_n. \tag{1}$$

特別令 $\beta=1$ 与 $\alpha_1 u_1+\cdots+\alpha_n u_n=u$, 即得

$$1\cdot u=u \tag{2}$$

由 3. 还推出

$$\begin{cases}(\alpha_1 u_1+\cdots+\alpha_n u_n)+(\beta_1 u_1+\cdots+\beta_n u_n)\\ \qquad=(\alpha_1+\beta_1)u_1+\cdots+(\alpha_n+\beta_n)u_n.\end{cases} \tag{3}$$

向量空間中每个元素 $u=\alpha_1 u_1+\cdots+\alpha_n u_n$ 唯一地被 n 个元素的序列 $(\alpha_1,\cdots,\alpha_n)$ 表示，它們称为 u（对于基 $u_1,\cdots,u_n$）的**分量**. 基元素或者分量的个数 n 称为向量空間的維数. 由(3), $\mathfrak{G}$ 中两个元素的相加就是它們分量的相加，用 β 去乘一个元素就是用 β 去乘它的分量.

向量空間在同构之下唯一地被环 $\mathfrak{R}$ 与維数 n 决定.

基于这个定理，对于給定的环 $\mathfrak{R}$ 我們可以取一个給定維数的空間作为所有同維数向量空間的模型. 最清楚的一个模型是：取 $\mathfrak{R}$ 中 n 个元素的序列 $(\alpha_1,\cdots,\alpha_n)$ 作为向量. 两个向量 $(\alpha_1,\cdots,\alpha_n)$ 与 $(\beta_1,\cdots,\beta_n)$ 的和定义为 $(\alpha_1+\beta_1,\cdots,\alpha_n+\beta_n)$, 乘积 $\beta(\alpha_1,\cdots,\alpha_n)$ 定义为 $(\beta\alpha_1,\cdots,\beta\alpha_n)$. 运算規律 1. 到 4. 自然适合. 再令

$$(1, 0, \cdots, 0) = u_1,$$
$$(0, 1, \cdots, 0) = u_2,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$(0, 0, \cdots, 1) = u_n,$$

于是

$$(\alpha_1, \cdots, \alpha_n) = (\alpha_1, 0, \cdots, 0) +$$
$$(0, \alpha_2, \cdots, 0) + \cdots + (0, 0, \cdots, \alpha_2)$$
$$= \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n,$$

所以 5. 也成立按照我們的定义，这些向量 $(\alpha_1, \cdots, \alpha_n)$ 确实組成一个 n 維向量空間。

为了由一个向量空間作出一个环，我們还必须对于元素 $u, v, \cdots$ 定义一个乘法。如果 $\mathfrak{R}$ 是交換的，那么可以按下面的方式进行：除去乘法的結合律与两条分配律之外我們再要求性質

(4) $$(\alpha u)v = u(\alpha v) = \alpha(uv) \quad 对于\ \alpha \in \mathfrak{R}.$$

如果这些性質全被滿足，那么环 $\mathfrak{S}$ 就称为环 $\mathfrak{R}$ 上的一个秩为 n 的**超复系**或者**代数**。在很多情形我們假定 $\mathfrak{R}$ 是域，但这并不是必須的。下面即将看到，我們怎样眞正地給出一个代数。

由 (4) 推出

$$(\alpha u)(\beta v) = (\alpha\beta)(uv)$$

以及

(5) $$\left(\sum_i \alpha_j u_j\right)\left(\sum_k \beta_k u_k\right) = \sum_i \sum_k \alpha_j \beta_k (u_j u_k).$$

因此一旦我們知道了乘积 $u_j u_k$，乘积 uv 就可以計算了。自然，乘积 $u_j u_k$ 又必須是 $u_1, \cdots, u_n$ 的綫性組合：

(6) $$u_j u_k = \sum_l \gamma^l_{jk} u_l.$$

按照 (5) 与 (6)，这 n^3 个常数 γ^l_{jk} 完全决定代数中的乘法，它們称

为代数的結构常数.

下面是定义代数的另一个方法. 在向量空間 $\mathfrak{S}$ 中选定一組基 $(u_1, \cdots, u_n)$, 首先按照 (6) 定义基元素的乘积, 然后按 (5) 来定义任意元素的乘积. 这样定义的乘法总是适合对加法的分配律. 在环的性質中只有乘法的結合律不是自然适合的. 只要基元素的乘积 $u_j u_k u_l$ 适合結合律, 即

$$(7)\qquad u_j(u_k u_l) = (u_j u_k) u_l,$$

那么任意元素

$$u = \sum_j \alpha_j u_j, \quad v = \sum_k \beta_k u_k, \quad w = \sum_l \gamma_l u_l$$

的乘积也就适合結合律. (7) 是对結构常数的一个附加条件. 如果它被适合, 那么公式 (1), (3), (5), (6) 就定义了环 $\mathfrak{R}$ 上的一个代数的运算. 这里甚至并不要求 $\mathfrak{R}$ 是交换的.

如果 $\mathfrak{R}$ 是交换的, 那么 (4) 可以由 (5) 推出. 在这个情形, 上面所給的代数的两个定义是等价的[1].

如果 $\mathfrak{S}$ 有单位元素 e, 那么 $\mathfrak{S}$ 中元素 αe 組成一个与 $\mathfrak{R}$ 同构的环; 因之它們可以与 $\mathfrak{R}$ 中的元素 α 等同起来.

如果 $\mathfrak{S}$ 是体, 那么 $\mathfrak{S}$ 也称为一可除代数.

例 1. 通常复数的定义.

取 $\mathfrak{R}$ 为实数域, e, i 代表一个二維向量空間的基元素, 乘积定义为

$$e \cdot e = e, \quad e \cdot i = i,$$
$$i \cdot e = i, \quad i \cdot i = -e.$$

基元素的乘法是交换的, 結合的; 因此 $\mathfrak{S}$ 是一个具有单位元素的

1) 如果 $\mathfrak{R}$ 不是交换的, 那么 (4) 只对于一些特殊的結构常数才成立. 見 G. Pickert: *Math. Ann.*, **120** (1948), 158.

交换环。元素 ae 可以与实数等同起来。元素 $ae+bi$ 就写成 $a+bi$。由于

$$(a-bi)(a+bi)=a^2+b^2>0 \quad (\text{除非 } a=b=0),$$

所以每个非零元素 $a+bi$ 都有逆，即 $(a^2+b^2)^{-1}(a-bi)$。因之，环 $\mathfrak{G}$ 是一个域，即复数域。

同样地，我們可以取 $\mathfrak{R}$ 为有理数域。这样得到的代数称为 Ganss 数域。如果取 $\mathfrak{R}$ 为有理整数的环，那么 $\mathfrak{G}$ 就是 Ganss 整数 $a+bi$ 的环。

例 2. 四元数体。$\mathfrak{R}$ 仍然是实数域或者有理数域，$\mathfrak{G}$ 是一个四維向量空間，基元素为 e, j, k, l，乘积公式为

$$ee=e; \quad jj=kk=ll=-e;$$

$$ej=je=j; \quad ek=ke=k; \quad el=le=l;$$

$$jk=l; \quad kj=-l;$$

$$kl=j; \quad lk=-j;$$

$$lj=k; \quad jl=-k,$$

它是結合的，但不交换。这样我們就得到一个具有单位元素的非交换环。元素 ae 与数 a 等同起来。元素 $a+bj+ck+dl$ 称为四元数。由于

$$(a-bj-ck-dl)(a+bj+ck+dl)=a^2+b^2+c^2+d^2,$$

所以每个非零的四元数 $a+bj+ck+dl$ 都有逆 $(a^2+b^2+c^2+d^2)^{-1}(a-bj-ck-dl)$。因之四元数組成一个体，称为四元数体。

例 3. 一个有限羣的羣环。如果取有限羣 $\mathfrak{g}$ 的元素作为一向量空間 $\mathfrak{R}_\mathfrak{g}$ 的基元素，那么結合律(7)是自然成立的。这样得到的代数 $\mathfrak{R}_\mathfrak{g}$ 称为 $\mathfrak{R}$ 上的 $\mathfrak{g}$ 的羣环。

习题. 1. 如果定义 n 阶矩陣为环 $\mathfrak{R}$ 中 n^2 个元素 $a_{jk}(j=1,\cdots,n;$

$k=1,\cdots,n$) 的元素組，并且按平常的方法定义两个矩陣 (α_{jk})，(β_{jk}) 的和 (σ_{jk}) 与积 (π_{jk}) 为

$$\sigma_{jk}=\alpha_{jk}+\beta_{jk},$$

$$\pi_{jk}=\sum_{l=1}^{n}\alpha_{jl}\beta_{lk},$$

那么这些 n 阶矩陣組成 $\Re$ 上的一个秩为 n^2 的代数。

2. 二阶复系数矩陣

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

組成一个与四元数体同构的代数。(利用这个事实可以比較簡单地証明四元数乘法的結合律。)

显然可以把代数的概念推广成秩为无穷的代数。考虑无穷多个基元素 $u_1, u_2, \cdots$，按(6)与(7)定义一个乘法。但是在推广的代数中，元素还只是有限和 $\Sigma\alpha_j u_j$。这一节所有的討論同样适用于"具有无穷基的代数"。

多項式环 $\Re[x]$ 是这种系統的最簡单的例子，下一节我們就来定义它。

§18. 多項式环

設 $\Re$ 是一环。用一个新的，不属于 $\Re$ 的符号 x 作表达式

$$f(x)=\sum a_\nu x^\nu,$$

这里是只对有限多个不同的整数 $\nu \geqq 0$ 求和，其中"系数" a_ν 属于 $\Re$；例如：

$$f(x)=a_0x^0+a_3x^3+a_5x^5.$$

这种表达式称为**多項式**；符号 x 称为**不定元**。因之不定元只是一个运算符号。两个多項式称为**相等**，如果它們除去系数为零的項外含有完全相同的項，而系数为零的項是允許任意删去和添进来的。

如果我們就按通常字母运算的規則把两个多項式 $f(x)$，$g(x)$ 相加或相乘，x 被認为是与环元素交換的并把 x 方次相同的項全合并起来，那么我們就得到一个多項式 $\sum c_\nu x^\nu$. 在加法的情形有

$$c_\nu = a_\nu + b_\nu, \tag{1}$$

在乘法的情形有

$$c_\nu = \sum_{\sigma+\tau=\nu} a_\sigma b_\tau. \tag{2}$$

現在我們用公式(1),(2)来定义两个多項式的和与积并且断言：

多項式組成一环.

加法的性質是显然的，因为它就归結为系数 a_ν，b_ν 的加法. 第一个分配律由

$$\sum_{\sigma+\tau=\nu} a_\sigma(b_\tau + c_\tau) = \sum_{\sigma+\tau=\nu} a_\sigma b_\tau + \sum_{\sigma+\tau=\nu} a_\sigma c_\tau$$

推出，相应地可以推出第二个分配律. 乘法的結合律由

$$\sum_{\alpha+\tau=\nu} a_\alpha\left(\sum_{\beta+\gamma=\tau} b_\beta c_\gamma\right) = \sum_{\alpha+\beta+\gamma=\nu} a_\alpha b_\beta c_\gamma,$$

$$\sum_{\rho+\gamma=\nu} \left(\sum_{\alpha+\beta=\rho} a_\alpha b_\beta\right) c_\gamma = \sum_{\alpha+\beta+\gamma=\nu} a_\alpha b_\beta c_\gamma$$

推出.

这个由 $\mathfrak{R}$ 得出的多項式环用 $\mathfrak{R}[x]$ 表示. 如果 $\mathfrak{R}$ 是交換的，則 $\mathfrak{R}[x]$ 也是.

一个非零多項式的**次数**就是使得 $a_\nu \neq 0$ 的最大的数 ν. 这个 a_ν 称为**首項系数**或者**最高項系数**.

零次多項式是 a_0x^0. 我們把这种多項式与基环 $\mathfrak{R}$ 中的元素 a_0 等同起来，这是可以的，因为按多項式的加法与乘法，它們組成一个与基环同构的系統(参看 § 15 最后). 因之多項式环 $\mathfrak{R}[x]$ 包含 $\mathfrak{R}$.

由 $\mathfrak{R}$ 造出 $\mathfrak{R}[x]$ 的方法称为**添加**（确切地，环添加）**一个不定**

元.

如果我們对环 $\mathfrak{R}$ 相継地添加不定元 $x_1, \cdots, x_n$，也就是作出 $\mathfrak{R}[x_1][x_2]\cdots[x_n]$，于是得出多項式环 $\mathfrak{R}[x_1, \cdots, x_n]$，它由所有的和

$$\sum a_{\alpha_1\cdots\alpha_n} x_1^{\alpha_1}\cdots x_n^{\alpha_n}$$

組成.

在这样的多項式中，因子 $x_1^{\alpha_1}, \cdots, x_n^{\alpha_n}$ 的次序是允許改变的. 这样，多項式环 $\mathfrak{R}[x_1][x_2]\cdots[x_n]$ 就与改变不定元的次序所得的多項式环，譬如說，$\mathfrak{R}[x_2][x_n]\cdots[x_1]$ 等同起来. 这样的等同是合理的，因 x_i 次序的改变对于和与积的定义沒有影响. $\mathfrak{R}[x_1, \cdots, x_n]$ 称为 n 个不定元 $x_1, \cdots, x_n$ 的多項式环.

如果 $\mathfrak{R}$ 特别是整数环，那么 $\mathfrak{R}[x]$ 就称为整系数多項式环.

不定元用任意的环元素代入. 如果 $f(x)=\sum a_\nu x^\nu$ 是 $\mathfrak{R}$ 上一多項式，α 是一个环元素（它是 $\mathfrak{R}$ 的或者是 $\mathfrak{R}$ 的一个扩环的元素），它与 $\mathfrak{R}$ 中所有元素交換，那么在 $f(x)$ 的表达式中可以用 α 来代 x，得到值 $f(\alpha)=\sum a_\nu \alpha^\nu$. 如果 $g(x)$ 是另一个多項式，$g(\alpha)$ 是 $x=\alpha$ 时的值，那么和与积

$$f(x)+g(x)=s(x), \quad f(x)\cdot g(x)=p(x)$$

对 $x=\alpha$ 的值为

$$f(\alpha)+g(\alpha)=s(\alpha), \quad f(\alpha)\cdot g(\alpha)=p(\alpha).$$

对于和，上面式子是显然的. 对于积，根据公式 (2) 有

$$p(\alpha)=\sum c_\nu \alpha^\nu=\sum_\nu \sum_{\lambda+\mu=\nu} a_\lambda b_\mu \alpha^\nu=\sum_\lambda \sum_\mu a_\lambda b_\mu \alpha^{\lambda+\mu}$$

$$=\left(\sum_\lambda a_\lambda \alpha^\lambda\right)\left(\sum_\mu b_\mu \alpha^\mu\right)=f(\alpha)g(\alpha).$$

因此我們証明了：多項式 $f(x), g(x), \cdots$ 之間所有通过加法与乘

法表示的关系在 x 用任意一个与 $\mathfrak{R}$ 中元素全交换的环元素 α 代入之后仍然保持.

对于多元多项式也有相应的定理. 特别是当 $\mathfrak{R}$ 交换时，多項式 $f(x_1, \cdots, x_n)$ 中的不定元可以用 $\mathfrak{R}$ 中(或者 $\mathfrak{R}$ 的一个交换扩环中)的任意元素代入. 基于这种代入的可能性,我們也称多項式为变元 $x_1, \cdots, x_n$ 的有理整函数.

对于沒有常数項的整系数多項式,代入的范围还可以扩大些: $x_1, \cdots, x_n$ 可以用任意一个环中互相交换的元素来代，不論这个环是否包含整数环在內.

如果 $\mathfrak{R}$ 是整环,则 $\mathfrak{R}[x]$ 也是一个整环.

証明. 如果 $f(x) \neq 0$ 与 $g(x) \neq 0$, a_α, b_β 分别是 $f(x)$, $g(x)$ 的最高項系数(不为零),那么 $a_\alpha b_\beta \neq 0$,它是 $f(x)\cdot g(x)$ 中 $x^{\alpha+\beta}$ 的系数;因之 $f(x)\cdot g(x) \neq 0$. 于是 $\mathfrak{R}[x]$ 中沒有零因子.

由証明还看出

推論. 如果 $\mathfrak{R}$ 是整环,那么 $f(x)\cdot g(x)$ 的次数等于 $f(x)$ 与 $g(x)$ 的次数的和.

对于 n 元多項式用完全归納法立即得出:

如果 $\mathfrak{R}$ 是整环,则 $\mathfrak{R}[x_1, \cdots, x_n]$ 也是整环.

項 $a_{\alpha_1\cdots\alpha_n}x_1^{\alpha_1}\cdots x_n^{\alpha_2}$ 的次数就是方次的和 $\sum\alpha_i$. 一个非零多項式的次数就是其中不为零的項的最大次数. 一个多項式称为齐次的或者称为一个齐式,如果它的項全有相同的次数,齐次多項式的乘积还是齐次多項式，当 $\mathfrak{R}$ 是整环时，乘积的次数等于因子次数的和.

非齐次多項式可以(唯一地)写成它的齐次部分的和. 当 $\mathfrak{R}$ 是整环时,如果两个次数分别为 m, n 的多項式 f, g 相乘，那么乘积的最高次的齐次部分是一非零的 $m+n$ 次齐式. $f\cdot g$ 中其它的

齐次部分次数都比它低；因之 $f\cdot g$ 的次数为 $m+n$. 因此上面的次数定理("推論")对多元多項式也对.

带余除法. 設 $\mathfrak{R}$ 是一具有单位元素的环,

$$g(x)=\sum c_\nu x^\nu$$

是首項系数 $c_n=1$ 的多項式,而

$$f(x)=\sum a_\nu x^\nu.$$

是任意一个次数 $m\geq n$ 的多項式，从 f 減去 g 的某个倍，譬如 $a_m x^{m-n}g$, 我們就消去了 f 的首項. 如果这样得出的多項式的次数还 $\geq n$,那么再減去 g 的一个倍就又消去首項. 这样一直下去,最后使余式的次数低于 n ,有

$$f-qg=r, \tag{3}$$

其中 r 是一个次数低于 g 的多項式或者是零. 这个手續称为带余除法.

特别如果 $\mathfrak{R}$ 是一个域并且 $g\neq 0$, 那么假定 $c_n=1$ 就不必要了;因为在必要时可以用 c_n^{-1} 乘 g 使首項系数变成 1.

习題. 如果 $x, y, \cdots$ 是无穷多个符号，我們可以考虑这些不定元的 $\mathfrak{R}$-多項式，但是每个多項式只能含有有限多个不定元. 証明：只要 $\mathfrak{R}$ 是环或者整环,則这些多項式也組成环或者整环.

§ 19. 理想. 同余类环

設 $\mathfrak{o}$ 是一个环.

$\mathfrak{o}$ 的一个子集合也是环($\mathfrak{o}$ 的子环)的充分必要条件为

1. 它是加法羣的一个子羣,換句話說，如果它包含 a, b, 就一定包含 $a-b$ (模性).

2. 如果包含 a, b, 就包含 ab.

在子环中有一些我們称为理想的起着重要的作用，它們类似

于羣論中的正規子羣。

$\mathfrak{o}$ 的一个非空子集合 $\mathfrak{m}$ 称为**理想**，或者确切地，**右理想**，如果

1. 由 $a \in \mathfrak{m}$ 与 $b \in \mathfrak{m}$ 推出 $a - b \in \mathfrak{m}$（模性）。

2. 由 $a \in \mathfrak{m}$，r 是 $\mathfrak{o}$ 中任意元素推出 $ar \in \mathfrak{m}$。 換句話說：如果模 $\mathfrak{m}$ 包含 a，就包含 a 的所有“右倍元” ar。

同样，一个模 $\mathfrak{m}$ 称为**左理想**，如果由 $a \in \mathfrak{m}$，对于任意的 $r \in \mathfrak{o}$ 推出 $ra \in \mathfrak{m}$。

如果 $\mathfrak{m}$ 既是左理想，又是右理想，它就称为**双边理想**。

对于交换环，这三个概念就重合了，我們簡单地称为**理想**。 在**这一节我們总假定 $\mathfrak{o}$ 是交換环**。理想总是用小写的德文字母代表。

理想的例子：

1. **零理想**，它由单个的零元素組成。

2. **单位理想**，它包含环中所有的元素。

3. **由元素 a 生成的理想** (a)，它由所有表成形式

$$ra + na \quad (r \in \mathfrak{o}, \quad n \text{ 整数})$$

的元素組成。 不难看出这个集合的确是理想：两个这种形式的元素的差还是这种形式，它的任意一个倍元

$$s\cdot(ra + na) = (sr + ns)\cdot a$$

具有形式 $r'a$，或者 $r'a + 0\cdot a$。

理想 (a) 显然是包含 a 的最小的（在包含关系下）理想；因为包含 a 的理想一定包含所有的倍数 ra 以及和 $\pm\sum a = na$，从而所有的和 $ra + na$。 因此理想 (a) 也可以定义为所有包含 a 的理想的交。

如果环 $\mathfrak{o}$ 有单位元素 e，那么 $ra + na$ 可以写成 $ra + nea = (r + ne)a = r'a$；**因之在这个情形，$(a)$ 是由所有的通常的倍元 ra 組成**。 例如，在整数环中理想 (2) 是由所有偶数組成。

由一个元素 a 生成的理想 (a) 称为**主理想**。零理想 (0) 总是主理想；当 $\mathfrak{o}$ 有单位元素 e，单位理想 $\mathfrak{o}$ 也是主理想，即 $\mathfrak{o}=(e)$。

4. 由元素 $a_1, \cdots, a_n$ 生成的理想同样可以定义为所有表成形式

$$\sum r_i a_i + \sum n_j a_j$$

的元素的集合，或者是所有包含元素 $a_1, \cdots, a_n$ 的理想的交。这个理想用 $(a_1, \cdots, a_n)$ 代表，$a_1, \cdots, a_n$ 称为一組**理想基**。

5. 同样可以定义由一个无穷集合 $\mathfrak{M}$ 生成的理想 $(\mathfrak{M})$；它是所有表成有限和

$$\sum r_i a_i + \sum n_j a_j \quad (a_i \in \mathfrak{M},\ r_i \in \mathfrak{o},\ n_j \text{ 整数})$$

的元素的全体。

同余类. 一个理想 $\mathfrak{m}$，作为环的加法羣的子羣，在 $\mathfrak{o}$ 中定义一个分类，把 $\mathfrak{o}$ 分成 $\mathfrak{m}$ 的陪集或者 $\mathfrak{m}$ 的**同余类**。两个元素 a, b 称为**对** $\mathfrak{m}$ **同余**或者**模** $\mathfrak{m}$ **同余**，如果它們属于相同的同余类，这就是說，$a-b \in \mathfrak{m}$。記为

$$a \equiv b (\bmod \mathfrak{m}),$$

或者簡写为

$$a \equiv b(\mathfrak{m}).$$

"a 不同余于 b" 写成 $a \not\equiv b$。

如果 $\mathfrak{m}$ 是一主理想 (m)，那么 $a \equiv b(\mathfrak{m})$ 也写成 $a \equiv b((m))$。在这个情形也可去掉一层括号簡写为 $a \equiv b(m)$。

通常的对于一个整数的同余式就是一个例子：$a \equiv b(n)$（讀为：a 同余于 b 模 n）就表示 $a-b$ 属于 (n)，也就是說，它是 n 的倍数。

同余式的計算. 如果用元素 c 加到一个对理想 $\mathfrak{m}$ 的同余式

$a \equiv b$ 的两边，或者用 c 乘同余式的两边，同余式显然仍成立。由此进一步推出：如果 $a \equiv a'$ 与 $b \equiv b'$，则

$$a + b \equiv a + b' \equiv a' + b',$$
$$ab \equiv ab' \equiv a'b';$$

因之同余式可以相加与相乘。

同余式的两边也可以用一个通常的整数 n 来乘。由 $n = -1$，再結合以上的結果就有：同余式可以相减。

因之同余式完全可以象方程一样計算。只是一般地不能消去公因子：例如，在整数中

$$15 \equiv 3(6),$$

但是虽然 $3 \not\equiv 0(6)$，并不能得出 $5 \equiv 1(6)$。

习题. 1. 証明：在整数环中理想 $(m)(m > 0)$ 的同余类可以用数 $0, 1, \cdots, m-1$ 来代表，因之可以用 $\mathfrak{K}_0, \mathfrak{K}_1, \cdots, \mathfrak{K}_{m-1}$ 表示。

2. 在整数环中数 10 与 13 合在一起生成的理想是什么？

3. $a \equiv b(0)$ 是什么意思？

4. 元素 a 的所有的倍元 ra 組成一个理想 $\mathfrak{o}a$。在偶数环中举例說明这个理想不一定与主理想 (a) 重合。

5. 对于非交换环定义由任意一个集合生成的右理想，左理想以及双边理想。

6. 在非交换环中同余式可以进行哪些运算？

理想与环同态的关系正如正规子羣与羣同态的关系一样。我們現在从同态的概念开始。

两个环的同态 $\mathfrak{o} \sim \bar{\mathfrak{o}}$ 定义了环 $\mathfrak{o}$ 的一个分类：类 $\mathfrak{K}_{\bar{a}}$ 是由所有以 $\bar{a}$ 为象元素的元素組成。这个分类我們現在可以較确切地刻划为：

$\mathfrak{o}$ 中在同态 $\mathfrak{o} \sim \bar{\mathfrak{o}}$ 下对应到零元素的类 $\mathfrak{n}$ 是 $\mathfrak{o}$ 的一个理想，其余的类都是这个理想的同余类。

証明. 首先 $\mathfrak{n}$ 是模。因为如果 a 与 b 在同态映射下变到零，

那么 $-b$ 也变到零，从而它們的差 $a-b$ 也变到零；所以随着 a 与 b 属于类 $\mathfrak{n}$ $a-b$ 也属于类 $\mathfrak{n}$.

$\mathfrak{n}$ 是理想；因为如果 a 变到零，r 是任意元素，那么 ra 变到 $\bar{r}\cdot 0=0$，所以 ra 也属于 $\mathfrak{n}$.

代表为 a 的同余类中的元素 $a+c(c\in\mathfrak{n})$ 变到 $\bar{a}+0=\bar{a}$，因之全属于一个类 $\mathfrak{R}_a$. 反过来，如果元素 b 变到 $\bar{a}$，那么 $b-a$ 变到 $\bar{a}-\bar{a}=0$；因而 $b-a\in\mathfrak{n}$，b 与 a 属于同一个同余类，这就完成了証明.

于是对于每一个同态都有一个理想作为它的核.

我們現在反过来看这个关系：从 $\mathfrak{o}$ 中一个理想 $\mathfrak{m}$ 出发，我們問，是不是有一个与 $\mathfrak{o}$ 同态的环 $\bar{\mathfrak{o}}$，它的元素恰好与 $\mathfrak{m}$ 的同余类对应.

为了造出这样一个环，我們和在 §13 中一样来作：我們就取 $\mathfrak{m}$ 的同余类作为要造的这个环的元素，同余类 $a+\mathfrak{m}$ 用 $\bar{a}$ 表示，同余类 $b+\mathfrak{m}$ 用 $\bar{b}$ 表示，定义 $\bar{a}+\bar{b}$ 为 $a+b$ 所在的同余类，$\bar{a}\cdot\bar{b}$ 为 $a\cdot b$ 所在的同余类. 如果 $a'\equiv a$ 是 $\bar{a}$ 中另一个元素，$b'\equiv b$ 是 $\bar{b}$ 中另一个元素，那么有[1]

$$a'+b'\equiv a+b,$$
$$a'\cdot b'\equiv a\cdot b;$$

因之 $a'+b'$ 与 $a+b$ 属于同一个同余类，$a'\cdot b'$ 与 $a\cdot b$ 属于同一个同余类. 由此可見，所給的和与积的定义不依賴于 $\bar{a}$, $\bar{b}$ 中元素 a, b 的选择.

每个元素 a 对应一个同余类 $\bar{a}$，这个对应是同态. 因为 $a+b$ 对应于和 $\bar{a}+\bar{b}$，ab 对应于积 $\bar{a}\bar{b}$，因之同余类組成一个环(§15).

---

1) 所有的同余式自然都是模 $\mathfrak{m}$ 的.

这个环称为 $\mathfrak{o}$ 对于理想 $\mathfrak{m}$ 或者 $\mathfrak{o}$ 模 $\mathfrak{m}$ 的同余类环 $\mathfrak{o}/\mathfrak{m}$。上面所給的对应把 $\mathfrak{o}$ 同态地映射到 $\mathfrak{o}/\mathfrak{m}$。在这个同态之下，理想 $\mathfrak{m}$ 与上面的 $\mathfrak{n}$ 有相同的地位。

这里我們看到了理想的重要性：利用它們可以造出与一个环同态的环。造出来的环的元素是一个理想的同余类。为了把两个同余类相乘或者相加，只要在同余类中任取两个代表相乘或者相加。由 $a \equiv b$ 推出 $\bar{a} = \bar{b}$：同余式在过渡到同余类环中变成了等式，$\mathfrak{o}$ 中同余式的运算对应于 $\mathfrak{o}/\mathfrak{m}$ 中等式的运算。

这样造出的与 $\mathfrak{o}$ 同态的环：同余类环 $\mathfrak{o}/\mathfrak{m}$ 基本上穷尽了所有与 $\mathfrak{o}$ 同态的环。如果 $\bar{\mathfrak{o}}$ 是 $\mathfrak{o}$ 的任意一个同态象，那么我們看到，$\bar{\mathfrak{o}}$ 的元素 1-1 地对应于一个理想 $\mathfrak{n}$ 的同余类。同余类 $\mathfrak{K}_a$ 对应 $\bar{\mathfrak{o}}$ 中元素 $\bar{a}$。同余类 $\mathfrak{K}_a$，$\mathfrak{K}_b$ 的和与积分别是 $\mathfrak{K}_{a+b}$ 与 $\mathfrak{K}_{ab}$；与它們对应的元素是

$$\overline{a+b} = \bar{a} + \bar{b}$$

$$\overline{ab} = \bar{a}\bar{b}.$$

因之同余类与 $\bar{\mathfrak{o}}$ 中元素的这个对应是一个同构。这就証明了：

每个与 $\mathfrak{o}$ 同态的环 $\bar{\mathfrak{o}}$ 都同构于一个同余类环 $\mathfrak{o}/\mathfrak{n}$。$\mathfrak{n}$ 是所有在 $\bar{\mathfrak{o}}$ 中象为零的元素組成的理想。反之，每个同余类环 $\mathfrak{o}/\mathfrak{n}$ 都是 $\mathfrak{o}$ 的一个同态象(环的同态定理)。

同余类环的例子. 在整数环中，对于一正整数 m 的同余类可以用 $\mathfrak{K}_0, \mathfrak{K}_1, \cdots, \mathfrak{K}_{m-1}$ 表示(参看习題 1)，这里 $\mathfrak{K}_a$ 是所有被 m 除余 a 的数組成的同余类。为了把同余类 $\mathfrak{K}_a$，$\mathfrak{K}_b$ 相乘或者相加，只要把它們的代表 a，b 相乘或者相加，然后化为它对于 m 的最小非負余数。

习題. 7. 虽然 $\mathfrak{o}$ 沒有零因子，同余类环 $\mathfrak{o}/\mathfrak{m}$ 还是可能有。在整数环中举一个例。

8. 同态 $\mathfrak{o}\sim\bar{\mathfrak{o}}$ 是同构的充分必要条件为 $\mathfrak{n}=(0)$.

9. 在域中除去零理想与单位理想外沒有其它理想,証明这个事实. 由此說明,域有哪些可能的同态象?

10. 在非交换环中,每个同态映射对应着一个双边理想,并且每个双边理想也都有一个同余类环.

11. Gauss 整数 $a+bi$ 的环(§17,例1)同构于 x 的整系数多项式环对于理想 (x^2+1) 的同余类环.

§20. 整除性. 素理想

設 $\mathfrak{b}$ 是环 $\mathfrak{o}$ 的一个理想(或者更一般地一个模). 如果 a 是 $\mathfrak{b}$ 的一个元素,那么我們写成 $a\equiv 0(\mathfrak{b})$ 并且說, a 被理想 $\mathfrak{b}$ 整除. 如果一个理想 $\mathfrak{a}$(或者一个模)的元素全被 $\mathfrak{b}$ 整除,我們就說 $\mathfrak{a}$ 被 $\mathfrak{b}$ 整除;这其实就是表示 $\mathfrak{a}$ 是 $\mathfrak{b}$ 的子集合,記为

$$\mathfrak{a}\equiv 0(\mathfrak{b}).$$

我們称 $\mathfrak{b}$ 是 $\mathfrak{a}$ 的一个因子, $\mathfrak{a}$ 是 $\mathfrak{b}$ 的一个倍理想. 因而,因子=包集合,倍理想=子集合. 如果又有 $\mathfrak{a}\neq\mathfrak{b}$, 即 $\mathfrak{a}\subset\mathfrak{b}$, $\mathfrak{b}$ 就称为 $\mathfrak{a}$ 的一个真因子, $\mathfrak{a}$ 是 $\mathfrak{b}$ 的一个真倍理想.

在具有单位元素的交换环中,对于主理想来說, $(a)\equiv 0((b))$ 就表示 $a=rb$, 于是理想論的整除性概念就变成了通常的整除性概念.

从现在开始所討論的环又假定都是交换的.

$\mathfrak{o}$ 中一理想 $\mathfrak{p}$ 称为素理想, 如果它的同余类环 $\mathfrak{o}/\mathfrak{p}$ 是一整环,也就是沒有零因子.

如果 $\mathfrak{p}$ 的同余类与以前一样还用加横表示,那么

由 $\overline{a}\overline{b}=0$ 与 $\overline{a}\neq 0$ 推出 $\overline{b}=0$.

或者同样地,对 $\mathfrak{o}$ 中任意 a, b, 由

$$ab\equiv 0(\mathfrak{p}),$$

$$a \not\equiv 0(\mathfrak{p})$$

推出

$$b \equiv 0(\mathfrak{p});$$

用文字来說就是：如果 $\mathfrak{p}$ 整除乘积，它一定整除其中一个因子.

显然，单位理想一定是素理想，因为条件 $a \not\equiv 0(\mathfrak{p})$ 是不可能被满足的. 零理想是素理想当且仅当环 $\mathfrak{o}$ 本身是一整环. 以后我們将看到，在整数环 C 中由一个素数生成的主理想也是素理想.

$\mathfrak{o}$ 中一理想称为极大的，如果除去 $\mathfrak{o}$ 本身外它不包含在其它的理想中，换句話說，它除去单位理想外沒有其它的眞因子. [例如，上面提到的 C 中素主理想 (p) 是极大的.]

在具有单位元素的环 $\mathfrak{o}$ 中，每一个不等于 $\mathfrak{o}$ 的极大理想 $\mathfrak{p}$ 一定是素理想，并且它的同余类环 $\mathfrak{o}/\mathfrak{p}$ 是域. 反之，如果 $\mathfrak{o}/\mathfrak{p}$ 是域，則 $\mathfrak{p}$ 极大.

証明. 在同余类环中我們要来解方程 $\bar{x}\bar{a} = \bar{b}$，其中 $\bar{a} \neq 0$. 設 $a \not\equiv 0(\mathfrak{p})$，$b$ 为任意元素，$\mathfrak{p}$ 与 a 生成一个理想，它是 $\mathfrak{p}$ 的一个眞因子(因为它包含 a)，于是它一定等于 $\mathfrak{o}$. 因之 $\mathfrak{o}$ 中任意的元素 b 都可以表成

$$b = p + ra \qquad (p \in \mathfrak{p},\ r \in \mathfrak{o}).$$

同态对应到同余类环中即得

$$\bar{b} = \bar{r}\bar{a},$$

从而方程 $\bar{x}\bar{a} = \bar{b}$ 就解出了.

因此这个同余类环是域. 由于域沒有零因子，所以 $\mathfrak{p}$ 是素理想.

反过来，如果 $\mathfrak{o}/\mathfrak{p}$ 是域，$\mathfrak{a}$ 是 $\mathfrak{p}$ 的一个眞因子，a 是 $\mathfrak{a}$ 中一个不属于 $\mathfrak{p}$ 的元素，那么同余式

$$ax \equiv b(\mathfrak{p})$$

对每个 b 在 $\mathfrak{o}$ 中都有解. 由此推出

$$ax \equiv b(\mathfrak{a}),$$
$$0 \equiv b(\mathfrak{a});$$

因为 b 是 $\mathfrak{o}$ 中任意元素,所以 $\mathfrak{a} = \mathfrak{o}$.

整数环中的零理想这个例子說明并不是每个素理想都是极大的,在整系数多項式环 $C[x]$ 中理想 (x) 也是这样一个例子,因为它以理想 $(2, x)$ 作为一个眞因子. 不难看出,理想 (x) 与 $(2, x)$ 都是素的.

习題. 1. 証明上面最后一句話.

2. 討論整数环中理想 (2), (3), 并証明它們都是素理想.

3. 对 Gauss 整数环 (§ 17, 例 1) 中理想 (3) 与 $(1 + i)$ 作同样的証明. 在这里,理想 (2) 是素的嗎?

最大公因子与最小公倍. 由两个理想 $\mathfrak{a}$, $\mathfrak{b}$ 的和生成的理想 $(\mathfrak{a}, \mathfrak{b})$ 称为这两个理想的*最大公因子*, 它是它們的公因子,并且每个公因子都除得尽它. $(\mathfrak{a}, \mathfrak{b})$ 也称为这两个理想的*和*, 因为它显然是由所有的元素 $a + b$ 組成,其中 $a \in \mathfrak{a}$, $b \in \mathfrak{b}$.

理想 $\mathfrak{a}$, $\mathfrak{b}$ 的交 $\mathfrak{a} \cap \mathfrak{b}$ 称为它們的*最小公倍*, 它是它們的公倍并且能整除它們的每个公倍.

§ 21. 欧几里得环与主理想环

定理. *在整数环 C 中每个理想都是主理想.*

証明. 設 $\mathfrak{a}$ 是 C 的一个理想. 如果 $\mathfrak{a} = (0)$, 結論是显然的. 如果 $\mathfrak{a}$ 包含一个数 $c \neq 0$, 那么它也包含 $-c$, 两者之中一定有一个是正的. 設 a 是理想 $\mathfrak{a}$ 中最小的正数.

如果 b 是理想中任一个数, r 是 b 被 a 除所得的余数,于是

$$b = qa + r, \quad 0 \leqslant r < a.$$

因为 a, b 都属于这个理想，所以 $b - qa = r$ 也属于它。由 $r < a$ 即得 $r = 0$；因为 a 是理想中最小的正数，因此 $b = qa$；这就是説，理想中所有的数全是 a 的倍数。由此得 $\mathfrak{a} = (a)$；即 $\mathfrak{a}$ 是主理想。

同样可以証明：

如果 $\mathbf{P}$ 是域，那么在多項式环 $\mathbf{P}[x]$ 中每个理想都是主理想。

不妨假定 $\mathfrak{a} \neq (0)$。在 $\mathfrak{a}$ 中取一个次数最低的多項式 a。因为在多項式环中有带余除法，所以理想中每个多項式都可表成

$$b = qa + r,$$

这里，如果 $r \neq 0$，它的次数就低于 a 的次数，这样，結論就可同样得到了。

一个具有单位元素的整环称为**主理想环**，如果其中每个理想都是主理想。以上我們証明了整数环 C 与多項式环 $\mathbf{P}[x]$ 是主理想环。

域显然是主理想环。因为如果域 $\mathbf{P}$ 的一个理想 $\mathfrak{a}$ 不是零理想，它必包含一个 $a \neq 0$，因而包含 $a^{-1} \cdot a = 1$；因此 $\mathfrak{a} = (1)$ 是零理想之外的唯一的理想(参看 §19 习題 9)。

在以上两个情形中所用的証明方法可以作如下的推广。設 $\mathfrak{R}$ 是一交换环，其中每个非零元素 a 都对应一个非負整数 $g(a)$，具有性質：

1. 对于 $a \neq 0, b \neq 0$ 有 $ab \neq 0$ 且 $g(ab) \geqslant g(a)$。

2. (带余除法)对于任意两个元素 a, b，其中 $a \neq 0$，有

$$b = qa + r,$$

这里 $r = 0$ 或者 $g(r) < g(a)$。

在 $\mathfrak{R} = C$ 的情形，令 $g(a) = |a|$，在 $\mathfrak{R} = \mathbf{P}[x]$ 的情形 $g(a)$ 是多項式 a 的次数。具有这个性質的环称为**欧几里得环**。利用以上对于 $\mathfrak{R} = C$ 与 $\mathfrak{R} = \mathbf{P}[x]$ 所用的証明方法即得定理：

在欧几里得环中每个理想都是主理想，即理想中的元素全是生成元 a 的倍元 qa.

特别，如果应用这个定理到单位理想，也就是整个的环上，那么存在一个元素 a，所有的环元素都是倍元 qa. 特别 a 本身也能表成：

$$a = ae.$$

由此推出，对于 $b = qa$:

$$qa = qae, \quad \text{也就是} \quad b = be.$$

这就証明了：

欧几里得环一定有单位元素.

欧几里得环中两个非零元素 a, b 生成的理想 (a, b) 是由所有形式为 $ra + sb$ 的元素組成，这个理想当然也是主理想，由一个元素 d 生成. 这就給出

$$d = ra + sb, \tag{1}$$

$$\begin{cases} a = gd, \\ b = hd. \end{cases} \tag{2}$$

根据 (2) d 是 a, b 的一个公因子，根据 (1) d 又是最大公因子，这就是說，a 与 b 的所有公因子全整除 d. 因之：在主理想环中，任意两个元素 a, b 都有一个最大公因子 d，它可以表成形式(1).

最大公因子通常用 $d = (a, b)$ 表示. 更确切地是 $(d) = (a, b)$，因为只是理想 (d)，而不是 d，被 a 与 b 所唯一决定. 如果 $(a, b) = 1$，那么 a 与 b 就称为沒有公因子的或者互素的.

上面的最大公因子的存在証明并沒有給出它的实际求法. 在欧几里得环中，最大公因子可以通过欧几里得已經給出的輾轉相除法(欧几里得算法[1]，由此才有欧几里得环的名称)来求.

---

1) 欧几里得，几何原本，第七篇，定理 1 与 2.

假設給了两个环元素 a_0, a_1, 其中 $g(a_1) \leqslant g(a_0)$. 于是按带余除法,有

$$a_0 = q_1a_1 + a_2, \quad g(a_2) < g(a_1),$$
$$a_1 = q_2a_2 + a_3, \quad g(a_3) < g(a_2).$$

再这样一直作下去,直到除出的余是零为止:

$$a_{s-1} = q_sa_s.$$

数 $a_0, a_1, a_2, \cdots, a_s$ 全可以表成形式 $ra_0 + ta_1$. a_s 的每一个因子(特别是 a_s 本身)按最后的等式也是 a_{s-1} 的因子,从而也是 a_{s-2} 的因子,最后它也是 a_1 与 a_0 的因子,因此 a_s 是 a_0 与 a_1 的最大公因子.

以上的考虑可以推广到非交换的情形;只是必須要求有左边的与右边的除法算式:

$$b = q_1a + r_1 = aq_2 + r_2, \quad g(r_1) < g(a), \quad g(r_2) < g(a).$$

于是推出,每个左理想都包含一个元素 a,理想中的元素全是 a 的左倍元 qa,同样每个右理想也有一个元素 a,理想中的元素全是 a 的右倍元 aq. 如果应用这个結論到单位理想上,那么就可以証明左单位元素与右单位元素的存在,从而单位元素存在.

与以上一样,最后可以証明两个元素 a, b 的左边的以及右边的最大公因子的存在.

在一体 $\mathbf{P}$ 上的多項式环 $\mathbf{P}[x]$ 是非交换的欧几里得环的一个最重要的例子.

习題. 1. 关系 $(a, b) = (d)$ 不因环 $\mathfrak{o}$ 扩张到任一个包环 $\bar{\mathfrak{o}}$ 而改变.

2. 欧几里得环中的可逆元素 ε 可以刻划为 $g(\varepsilon) = g(1)$.

3. 假如数 r 与 s 互素,即 $(r, s) = 1$. 羣 $\mathfrak{G}$ 中任一个阶为 $r \cdot s$ 的元素 a 都是一个唯一决定的阶为 s 的方冪 $a^{\lambda r}$ 与一个唯一决定的阶为 r 的方冪 $a^{\mu s}$ 的乘积.

4. 如果 a 是一个阶为 n 的循环羣的生成元,那么所有的方冪 a^{μ} 也是生成元. 其中 $(\mu, n) = 1$.

欧几里得环的又一个例子. 我們来考虑 Gauss 整数 $a + bi$ 組成的环(§ 17, 例 1).

由乘法的定义

$$(a+bi)(c+di)=(ac-bd)+(ad+bc)i$$

推出,如果我們定义数 $\alpha=a+bi$ 的"模"为

$$N(\alpha)=(a+bi)(a-bi)=a^2+b^2,$$

那么就有等式

$$N(\alpha\beta)=N(\alpha)N(\beta). \tag{3}$$

模 $N(\alpha)$ 是一个通常的整数,只有当 α 为零时它才为零,否则总是正的(它是平方和). 由 (3) 可知,只有 α 或者 β 为零,乘积 $\alpha\beta$ 才能为零;因之它是一个整环.

根据 § 16,它有一个商域. 如果 $\alpha=a+bi\neq 0$, 那么 $\alpha^{-1}=\dfrac{a-bi}{N(\alpha)}$;因之商域中的元素全可以表成形式 $\dfrac{a}{n}+\dfrac{b}{n}i$($a$, b, n 是整数). 这些"分数"組成"Gauss 数域". 对于这个域中的元素完全一样地有模的定义与等式(3).

为了証明 Gauss 整数环有带余除法,我們对于給定的数 α 与 $\beta\neq 0$ 来找一个数 $\alpha-\lambda\beta$,它比 β 有較小的模. 首先我們取一个分数 $\lambda'=a'+b'i$ 使 $\alpha-\lambda'\beta=0$;然后取分別与 a', b' 最近的整数 a, b,令 $\lambda=a+bi$, $\lambda'-\lambda=\varepsilon$. 于是有

$$\alpha-\lambda\beta=\alpha-\lambda'\beta+\varepsilon\beta=\varepsilon\beta,$$

$$N(\alpha-\lambda\beta)=N(\varepsilon)N(\beta),$$

$$N(\varepsilon)=N(\lambda'-\lambda)=(a'-a)^2+(b'-b)^2\leqslant\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2<1,$$

$$N(\alpha-\lambda\beta)<N(\beta).$$

这就証明了带余除法,从而这个环是欧几里得环.

习题. 5. 按同样的方法討論由数 $a+b\rho$ 組成的环,其中 a, b 为任意整数,而 ρ 适合方程

$$\rho^2=-\rho-1.$$

同样討論由数 $a+b\sqrt{2}$; $a+b\sqrt{-2}$ 組成的环. 为什么对于 $a+b\sqrt{-3}$ 与 $a+b\sqrt{-5}$ 这个方法不行? 在第一个提出来的环中,理想 $(2, 1+\sqrt{-3})$ 是不是主理想?

文献. 关于是否在任意的主理想环中都有欧几里得算法或者广义的欧几里得算法的問題,参看 H. Hasse: *J. reine u. angew. Math.*, **159** (1928), 3—12. 关于在哪些代数数环中有欧几里得除法的問題, O. Perron (*Math.*

Ann., **107**, 489), A. Oppenheim (*Math. Ann.*, **109**, 349), E. Berg (*Kgl. Fysiogr. Sällskapets Lund Förhandl.* **5**, N5), N. Hofreiter (*Mh. Math. Physik*, **42**, 397), H. Behrbohm 与 L. Redei (*J. reine u. angew. Math.*, **174**, 198)都曾經研究过.

§22. 因子分解

在这一节我們只考虑具有单位元素的整环. 首先我們来看一下,在这样的环中如何定义素元素(或者不可分解元素)比較合适. 在討論中,我們只考虑环中非零元素,这一点就不到处声明了.

在整数环中通常的素数总有以下两种分解:

$$p = p\cdot 1 = (-p)\cdot(-1).$$

在分解中一定有一个因子是"可逆元素",所謂可逆元素就是逆 ε^{-1} 也在整数环中的数 ε. $+1$ 与 -1 是可逆元素.

如果一般地给了一个具有单位元素的整环, 那么在环中有逆元素 ε^{-1} 的元素 ε 称为**可逆元素**[1]. 显然 ε^{-1} 也是可逆元素.

每个元素 a 总有分解

$$a = a\varepsilon^{-1}\cdot\varepsilon,$$

其中 ε 是一个可逆元素. 我們可以称这种以可逆元素作为一个因子的分解为"平凡的分解".

如果一个元素 p 只有平凡的分解,即由 $p = ab$ 推出 a 或 b 是一可逆元素,它就称为**素元素**. (对于整数就是**素数**;对于多項式就是**不可約多項式**.)

两个只差一个可逆元素作为因子的元素 a 与 $b = a\varepsilon^{-1}$ 常常被称为"相伴的元素". 它們之中的每一个都是另一个的因子. 对于

---

1) 在原文中,可逆元素是 Einheit, 单位元素是 Einselement, 它們常常作为同意詞来用. 但是在因子分解的討論中, 二者必須严格区分.

所属的主理想有

$$(a) \subseteq (b), \quad (b) \subseteq (a), \quad 从而 \quad (a) = (b);$$

因之相伴的元素生成相同的主理想.

反之,如果两个元素 a, b 互为因子:

$$a = bc, \quad b = ad.$$

那么

$$b = bcd, \quad 从而 \quad 1 = cd, \quad c = d^{-1},$$

因之 c 与 d 是可逆元素, a 与 b 是相伴的.

如果 c 是 a 的一个因子,但不与 a 相伴, 卽 $a = cd$, d 不是可逆元素,那么 c 就称为 a 的一个眞因子. 在这个情形, a 就不是 c 的因子,理想 (c) 是理想 (a) 的一个眞因子. 否則,假如 a 是 c 的因子,卽 $c = ab$, 于是

$$a = cd = abd,$$

$$1 = bd,$$

d 就要是可逆元素了.

素元素現在也可以定义为一个非零元素, 它除去可逆元素外沒有眞因子.

在欧几里得环中,如果 b 是 a 的一个眞因子,則 $g(b) < g(a)$.

証明. 用 a 除 b 有

$$b = aq + r, \quad g(r) < g(a).$$

以 $a = bc$ 代入,卽得

$$r = b - aq = b(1 - cq),$$

$$g(r) \geqslant g(b), \quad 从而 \quad g(b) \leqslant g(r) < g(a).$$

在欧几里得环中每个非零元素 a 都可以分解成素元素的連乘积:

$$a = p_1 p_2 \cdots p_r.$$

証明. 我們对 $g(a)$ 作完全归納法: 假定結論对于所有的

$g(b) < n$ 的元素 b 已經成立，而 $g(a) = n$. 如果 a 是素元素：$a = p$，那么沒有什么可証的. 如果 a 可以分解：$a = bc$，其中 b 与 c 都是 a 的眞因子，那么

$$g(b) < g(a), \quad g(c) < g(a).$$

按归納假定，b 与 c 都是素元素的乘积. 因之 $a = bc$ 也是素元素的乘积.

我們現在来討論素因子分解 $a = p_1 p_2 \cdots p_r$ 的唯一性究竟怎样，討論不限于欧几里得环，也包括一般的主理想环.

在主理想环中，一个非可逆的不可分解元素生成极大素理想（它的同余类环因之是域）.

証明. 如果 p 不可分解，那么 p 除去可逆元素外沒有其他的眞因子，也就是（因为每个理想都是主理想）理想 (p) 除去单位理想外沒有眞理想因子.

注意. 在同余类环中方程 $ax = b$ 或者在原来环中同余式 $ax \equiv b(p)$ 的可解性自然也可以由以下事实推出，由 $a \not\equiv 0(p)$ 必有 $(a, p) = 1$，于是

$$1 = ar + ps,$$
$$b = arb + psb,$$
$$b \equiv arb(p).$$

一个直接的推論是：

如果素元素 p 整除一个乘积，它一定整除其中一个因子；因为这个同余类环沒有零因子.

习題. 1. 利用欧几里得算法解同余式

$$6x \equiv 7(19).$$

2. 在整数模 (19) 的同余类环中，6 的同余类的逆是什么？

現在已經可以来証明**在主理想环中的素因子分解唯一性定理**.

設

$$a = p_1p_2\cdots p_r = q_1q_2\cdots q_s \tag{1}$$

是元素 a 在主理想环中的两个分解. 我們把 a 是可逆元素这个平凡的情形除外,这时所有的 p_i 与 q_j 自然都是可逆元素. 我們可以假定 p_1 与 q_1 不是可逆元素并且在 p_i 与 q_j 中所有的可逆元素都与 p_1, q_1 合并起来. 这样,可設 p_i 与 q_j 中沒有可逆元素. 現在我們断言: $r = s$ 并且除去次序与差一个可逆的因子外, p_i 与 q_j 完全一样.

对于 $r = 1$ 結論是显然的;因为根据 $a = p_1$ 的不可分解性,乘积 $q_1\cdots q_s$ 只能包含一个因子 $q_1 = p_1$. 对 r 作完全归納法. 因为 p_1 整除乘积 $q_1\cdots q_s$, 它必然整除其中一个 q_j. 重新排列次序可令 p_1 整除 q_1:

$$q_1 = \varepsilon_1 p_1. \tag{2}$$

这里 ε_1 必須是可逆元素,否则 q_1 就不是素元素了. 把(2)代入(1)并消去 p_1 得

$$p_2\cdots p_r = (\varepsilon_1 q_2)q_3\cdots q_s. \tag{3}$$

按归納假定,(3)中两端的因子除去差可逆因子外重合. 因为 p_1 与 q_1 也只差一个可逆因子,这就完成了証明.

由所証的定理推出:欧几里得环中的元素,除去因子的次序以及差可逆因子外,可以唯一地表成素元素的乘积. 特別地,这个定理在整数环中,在系数在域中的一元多项式环中以及在 Gauss 整数环中是成立的.

习題. 3. 整系数多項式 $f(x)$ 模素数 p 可以唯一地表成模 p 的不可分解因子的乘积.

4. Gauss 数环中可逆元素是什么? 在这个环中把 2, 3, 5 分解成素因子的乘积.

5. 在数 $a + b\sqrt{-3}$ 組成的环中, 4 有两个本質上不同的素因子分解:

$$4=2\cdot2=(1+\sqrt{-3})(1-\sqrt{-3}).$$

6. 在主理想环中，由与元素 a 互素的元素組成的模 a 的同余类在乘法下成一羣。

在下一章將看到，唯一因子分解定理在一些非主理想的环中也成立。对于所有这样的环我們現在証明定理：

如果 $\mathfrak{o}$ 中每个元素可以唯一地分解成素元素的乘积，那么每个不可分解元素生成一素理想，每个非零的可分解元素不生成素理想。

証明. 設 p 不可分解. 如果 $ab\equiv0(p)$，那么 p 一定出現在 ab 的分解中. 把 a 与 b 的因子分解合在一起就得到 ab 的因子分解；因之 p 一定出現在 a 的分解中或者 b 的分解中，卽 $a\equiv0(p)$ 或者 $b\equiv0(p)$.

現在設 p 可分解：$p=ab$，a,b 是 p 的眞因子. 于是 $ab\equiv0(p)$ 而 $a\not\equiv0(p)$，$b\not\equiv0(p)$. 理想 (p) 不是素理想.

习題. 7. 証明：在具有唯一因子分解的环中，任意两个或多个元素都有一个“最大公因子”与一个“最小公倍”，它們除可逆因子外是唯一决定的.

注意. 在这种环中，元素意义的最大公因子与理想意义的最大公因子不一定一致. 例如，在整系数一元多項式环中，元素 2 与 x 除去可逆元素外沒有公因子；但是理想 $(2,x)$ 并不是单位理想.（下一章将証明，在这个环中有唯一的因子分解.）

第四章　有理整函数

內容.　关于系数在一个交换环 $\mathfrak{o}$ 或域 Σ 中的一元及多元多項式的簡单定理.

§23. 微　分　法

在这一节里,将不用連續性思想对于任意多項式环 $\mathfrak{o}[x]$ 来定义有理整函数的微商.

令 $f(x)=\sum a_i x^i$ 是 $\mathfrak{o}[x]$ 中任意一个多项式. 在一个多項式环 $\mathfrak{o}[x, h]$ 中作多項式 $f(x+h)=\Sigma a_i(x+h)^i$, 并且依 h 的冪展开,于是得

$$f(x+h)=f(x)+hf_1(x)+h^2f_2(x)+\cdots,$$

或

$$f(x+h)\equiv f(x)+h\cdot f_1(x)(\bmod h^2).$$

h 的一次冪的(唯一确定)系数 $f_1(x)$ 叫做 $f(x)$ 的导数, 通常記作 $f'(x)$. $f'(x)$ 显然也可以这样得到:作差 $f(x+h)-f(x)$, 用其中所含的有理整因子 h 去除,然后在所得的多項式中令 $h=0$. 由此易見,当 $\mathfrak{o}$ 就是实数域时,导数的定义与通常把 $\lim\limits_{h\to 0}\dfrac{f(x+h)-f(x)}{h}$ 作为微商的定义是一致的. 因此导数也可以記作 $\dfrac{df}{dx}$ 或 $\dfrac{d}{dx}f(x)$, 或者当 f 除 x 外还含有其它变元时,記作 $\partial f/\partial x$.

下列运算規則成立:

(1)　　$(f+g)'=f'+g'$　(和規則).

(2) $$(fg)' = f'g + fg' \quad \text{(积規則)}.$$

証明 (1):

$$f(x+h)+g(x+h) \equiv f(x)+hf'(x)+g(x)+hg'(x) \pmod{h^2}.$$

証明 (2):

$$f(x+h)g(x+h) \equiv \{f(x)+hf'(x)\}\{g(x)+hg'(x)\}$$
$$\equiv f(x)g(x) + h\{f'(x)g(x)+f(x)g'(x)\} \pmod{h^2}.$$

同样可証一般的:

(3) $$(f_1 + \cdots + f_n)' = f_1' + f_2' + \cdots + f_n',$$

(4) $$(f_1 f_2 \cdots f_n)' = f_1' f_2 \cdots f_n + f_1 f_2' \cdots f_n + \cdots + f_1 f_2 \cdots f_n'.$$

由 (4) 进一步推出

(5) $$(ax^n)' = nax^{n-1}.$$

由 (3) 及 (5) 推出

$$\left(\sum_0^n a_k x^k\right)' = \sum_0^n k a_k x^{k-1}.$$

通过这些公式,微商也可以形式地定义.

习题. 1. 設 $F(z_1, \cdots, z_m)$ 是一个多項式而 $F_\nu = \partial F/\partial z_\nu$. 証明公式

$$\frac{d}{dx} F(f_1(x), \cdots, f_m(x)) = \sum_1^m F_\nu(f_1, \cdots, f_m) \frac{df_\nu}{dx}.$$

2. 对于 r 次齐次多項式 $f(x_1, \cdots, x_n)$, 由方程

$$f(hx_1, \cdots, hx_n) = h^r f(x_1, \cdots, x_n)$$

推导 "Euler 微分方程":

$$\sum_\nu \frac{\partial f}{\partial x_\nu} x_\nu = rf.$$

3. 給出系數在一个域內的有理分函数 $f(x)/g(x)$ 的导数的代数定义, 并且証明关于和、积及商的微分法的熟知的运算規則.

§24. 零　　点

令 $\mathfrak{o}$ 是一个有单位元素的整环.

$\mathfrak{o}$ 的一个元素 α 叫做 $\mathfrak{o}[x]$ 中一个多项式 $f(x)$ 的**零点**或**根**，如果 $f(\alpha)=0$. 下列定理成立:

若 α 是 $f(x)$ 的一个零点，则 $f(x)$ 可以被 $x-\alpha$ 整除.

証明. 以 $x-\alpha$ 除 $f(x)$ 得到

$$f(x)=q(x)\cdot(x-\alpha)+r,$$

此处 r 是一个常数. 以 $x=\alpha$ 代入得

$$0=r,$$

从而

$$f(x)=q(x)\cdot(x-\alpha).$$

假若 $\alpha_1,\cdots,\alpha_k$ 是 $f(x)$ 的不同的零点，則 $f(x)$ 能被乘积 $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)$ 整除.

証明. 对于 $k=1$，定理刚才已經被証明. 假設定理已經对于值 $k-1$ 被証明，那末有

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_{k-1})g(x);$$

以 $x=\alpha_k$ 代入，得

$$0=(\alpha_k-\alpha_1)\cdots(\alpha_k-\alpha_{k-1})g(\alpha_k),$$

因为 $\mathfrak{o}$ 沒有零因子又 $\alpha_k\neq\alpha_1,\cdots,\alpha_k\neq\alpha_{k-1}$，所以

$$g(\alpha_k)=0,$$

于是由上面的定理:

$$g(x)=(x-\alpha_k)\cdot h(x),$$

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_{k-1})(x-\alpha_k)h(x). \text{ 証毕.}$$

推論. 一个异于零的 n 次多项式在一个整环中至多有 n 个零点.

这一命題在一个沒有单位元素的整环中也成立，因为这样的一个整环总可以嵌入一个域(有单位元)內. 然而它在有零因子的环中不成立；例如，在模 16 的同余类环內，多项式 x^2 有零点 0, 4,

8, 12, 并且甚至还有这样的环，在其中这个多項式有无穷多个零点(§ 14,习題 3). 对于非交換环,这一命題也不成立,因为在四元数体(§ 17,例 2)內，多項式 x^2+1 有零点 $\pm i$, $\pm j$, $\pm k$(并且还有无穷多个).

若 $f(x)$ 能被 $(x-\alpha)^k$ 整除,但不能被 $(x-\alpha)^{k+1}$ 整除, 那末就称 α 为 $f(x)$ 的一个 k 重零点(或 k 重根). 我們有

$f(x)$ 的一个 k 重零点对它的导数 $f'(x)$ 来說至少是一个$(k-1)$重零点.

証明. 由 $f(x)=(x-\alpha)^k g(x)$ 推出

$$f'(x)=k(x-\alpha)^{k-1}g(x)+(x-\alpha)^k g'(x),$$

从而 $f'(x)$ 能被 $(x-\alpha)^{k-1}$ 整除.

同样可以証明: $f(x)$ 的一个单零点不再是导数 $f'(x)$ 的零点.

我們現在轉向关于多元多項式的零点的一些定理.

如果多項式 $f(x_1,\cdots,x_n)$ 不为零,并且对于不定元 $x_1,\cdots,x_n$ 的每一个都有一个无限集供它取值，而这些无限集包含在 $\mathfrak{o}$ 或包含在一个包含 $\mathfrak{o}$ 的整环中,那末至少有一組值 $x_1=\alpha_1$, $x_2=\alpha_2$, $\cdots$, $x_n=\alpha_n$,使得 $f(\alpha_1,\cdots,\alpha_n)\neq 0$.

証明. $f(x_1,\cdots,x_n)$ 作为 x_n 的多項式(系数是在整环 $\mathfrak{o}[x_1,\cdots,x_{n-1}]$ 內), 至多有有限个零点; 因此在供 x_n 选取的值的无限集中,有一个值 α_n 使得

$$f(x_1,\cdots,x_{n-1},\alpha_n)\neq 0.$$

把这个表示式作为 x_{n-1} 的多項式处理;于是有一个值 α_{n-1} 使得

$$f(x_1,\cdots,x_{n-2},\alpha_{n-1},\alpha_n)\neq 0.$$

如此等等.

推論. 如果对于一个无限整环中一切特殊值 x_i 来說,多項式 $f(x_1,\cdots,x_n)$ 的值都是零,那末它("恆等地")等于零.

应該注意，在代数里，关于 $x_1, \cdots, x_n$ 的多項式等于零意味着它的一切系数都等于零，而不是說对于 $x_1, \cdots, x_n$ 可能取的一切值，多項式的值都是零． 因此方才所建立的定理并不是同語的反复．

习题． 把最后这个定理推广到一組有限个多項式 $f_i(x_1, \cdots, x_n)$ 上，其中每一个多項式都不恆等于零．

§25. 內插公式

我們仍回到一元多項式上，但假定它的系数区域是一个域．根据已証明的定理，如果两个次数 $\leqslant n$ 的多項式在 $n+1$ 个点上的值相同，那末它們彼此相等；因为它們的差有 $n+1$ 个零点而最高是 n 次的． 因此至多存在一个多項式，它在 $n+1$ 个不同的点 $\alpha_0, \cdots, \alpha_n$ 取給定的值 $f(\alpha_i)$． 另一方面，总存在一个次数 $\leqslant n$ 的多項式，它在这些点取所給定的值，就是多項式

$$(1)\quad f(x)=\sum_{i=0}^{n}\frac{f(\alpha_i)(x-\alpha_0)\cdots(x-\alpha_{i-1})(x-\alpha_{i+1})\cdots(x-\alpha_n)}{(\alpha_i-\alpha_0)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_n)}.$$

这样，存在而且只存在一个次数 $\leqslant n$ 的多項式，它在 $n+1$ 个点 α_i 取給定的值 $f(\alpha_i)$，这个多項式由公式 (1) 給出． 公式 (1) 叫做 Lagrange 內插公式．

具有所希望的性质的一个多項式也可以通过 Newton 內插公式

$$(2)\quad \begin{cases} f(x) = \lambda_0+\lambda_1(x-\alpha_0)+\lambda_2(x-\alpha_0)(x-\alpha_1)+\cdots+ \\ \qquad +\lambda_n(x-\alpha_0)(x-\alpha_1)\cdots(x-\alpha_{n-1}) \end{cases}$$

得到，此处系数 $\lambda_0, \cdots, \lambda_n$ 依次通过代入值 $x=\alpha_0, \cdots, x=\alpha_n$ 来确定．

最好按下面的方式进行計算：首先在 (2) 中令 $x=\alpha_0$ 而得到

$$f(\alpha_0)=\lambda_0.$$

由 (2) 减去它并且用 $x-\alpha_0$ 去除，于是得

$$(3)\qquad \frac{f(x)-f(\alpha_0)}{x-\alpha_0}=\lambda_1+\lambda_2(x-\alpha_1)+\cdots+ \\ +\lambda_n(x-\alpha_1)\cdots(x-\alpha_{n-1}).$$

把左端称做 $f(\alpha_0, x)$. 在 (3) 中令 $x=\alpha_1$，我們有

$$f(\alpha_0, \alpha_1)=\lambda_1.$$

由 (3) 减去它并且用 $x-\alpha_1$ 去除，得

$$\frac{f(\alpha_0, x)-f(\alpha_0, \alpha_1)}{x-\alpha_1}=\lambda_2+\lambda_3(x-\alpha_2)+\cdots+ \\ +\lambda_n(x-\alpha_2)\cdots(x-\alpha_{n-1}).$$

把左端称作 $f(\alpha_0, \alpha_1, x)$. 令 $x=\alpha_2$ 得

$$f(\alpha_0, \alpha_1, \alpha_2)=\lambda_2.$$

按这个方式継續下去. 一般，令(根据完全归納定义)

$$(4)\quad f(\alpha_0, \cdots, \alpha_k, x)=\frac{f(\alpha_0,\cdots,\alpha_{k-1},x)-f(\alpha_0,\cdots,\alpha_{k-1},\alpha_k)}{x-\alpha_k},$$

并且如上求得

$$f(\alpha_0, \cdots, \alpha_{k-1}, x)=\lambda_k+\lambda_{k+1}(x-\alpha_k)+\cdots+ \\ +\lambda_n(x-\alpha_k)\cdots(x-\alpha_{n-1}),$$

$$(5)\qquad f(\alpha_0, \cdots, \alpha_k)=\lambda_k.$$

$f(\alpha_0, \cdots, \alpha_k)$ 叫做函数 $f(x)$ 对于点 $\alpha_0, \cdots, \alpha_k$ 的 k 次差商. 由 (4) 有

$$(6)\quad \begin{cases} f(\alpha_0,\alpha_1)=\dfrac{f(\alpha_1)-f(\alpha_0)}{\alpha_1-\alpha_0}, \\ f(\alpha_0,\alpha_1,\alpha_2)=\dfrac{f(\alpha_0,\alpha_2)-f(\alpha_0,\alpha_1)}{\alpha_2-\alpha_1}, \\ f(\alpha_0,\cdots,\alpha_n)=\dfrac{f(\alpha_0,\cdots,\alpha_{n-2},\alpha_n)-f(\alpha_0,\cdots,\alpha_{n-2},\alpha_{n-1})}{\alpha_n-\alpha_{n-1}}. \end{cases}$$

k 次差商也可以定义为一个次数 $\leqslant k$ 的多項式 $\varphi_k(x)$ 中 x^k 的系

数，这个多项式在点 $\alpha_0, \cdots, \alpha_k$ 上取值 $f(\alpha_0), \cdots, f(\alpha_k)$. 根据 Newton 内插公式,这个多项式由

$$\varphi_k(x) = \lambda_0 + \lambda_1(x-\alpha_0) + \cdots + \lambda_k(x-\alpha_0)\cdots(x-\alpha_{k-1})$$

給出. 而在这个表达式中 x^k 的系数正好是 $\lambda_k = f(\alpha_0, \cdots, \alpha_k)$.

由最后給出的定义推出，k 次差商不依賴于点 $\alpha_0, \cdots, \alpha_k$ 的順序(即号碼). 这个性質在实际計算时可以如此加以利用,即当 $\alpha_0, \cdots, \alpha_k$ 是作为有理数按自然順序給出时，差商永远仅对邻接点 α_ν 作出,并且用公式

$$(7) \qquad f(\alpha_0, \alpha_1, \cdots, \alpha_k) = \frac{f(\alpha_1, \cdots, \alpha_k) - f(\alpha_0, \cdots, \alpha_{k-1})}{\alpha_k - \alpha_0}$$

代替公式(6)，这个公式是在公式(6)中交换 α_ν 而得到的. 于是差商可以按以下方法排列成一个格式:

$$\begin{array}{lllll}
f(\alpha_0) & & & & \\
 & f(\alpha_0, \alpha_1) & & & \\
f(\alpha_1) & & f(\alpha_0, \alpha_1, \alpha_2) & & \\
 & f(\alpha_1, \alpha_2) & & & \cdots\cdots \\
f(\alpha_2) & & f(\alpha_1, \alpha_2, \alpha_3) & & \\
 & f(\alpha_2, \alpha_3) & \cdots\cdots\cdots & & \\
f(\alpha_3) & \cdots\cdots & & & \\
\cdots & & & &
\end{array}$$

根据(7)，每一个后面的列都是由它前一列作一阶差商而构成的. 如果还有新的点出現,这个格式可以任意向下継續. 如果 $f(x)$ 是一个 n 次多項式，那末第 n 列中都是常数，即 x^n 的系数 λ_n. 这时在第 $n+1$ 列中全是零.

高阶算术数列. 我們假定基域包含有理数域并且点 $\alpha_0, \alpha_1, \alpha_2, \cdots$ 取作相邻的整数，例如 $0, 1, 2, \cdots$. 作出上面的差商格式，那末根据(7)出現在第 $k+1$ 列差商中的分母 $\alpha_k - \alpha_0$, $\alpha_{k+1} - \alpha_1, \cdots$ 都等于 k. 把第二列乘以 1，第三列乘以 2，第四列乘以 $2\cdot3$,一般,第 $k+1$ 列乘以 $k!$,那末代替差商格式,我們得到

差分格式：

$$
(8)\qquad \begin{cases}
b_0 & & & \\
& \Delta b_0 & & \\
b_1 & & \Delta^2 b_0 & \\
& \Delta b_1 & & \cdots \\
b_2 & & \Delta^2 b_1 & \\
& \Delta b_2 & \vdots & \\
b_3 & \vdots & & \\
\vdots & & &
\end{cases}
$$

在其中令 $f(a_\nu)=b_\nu$. Δb_ν 表示 $b_{\nu+1}-b_\nu$; $\Delta^2 b_\nu$ 表示 $\Delta\Delta b_\nu=\Delta b_{\nu+1}-\Delta b_\nu$, 等等. 若 $b_0, b_1, \cdots$是一个 n 次多項式的值,那末根据上述, n 次差分是常数而 $n+1$ 次差分是零. 这个多項式本身由公式 (2) 給出,其中

$$
(9)\qquad \lambda_k=\frac{\Delta^k b_0}{k!}.
$$

这一命題的逆命題也成立:

若序列 $b_0, b_1, b_2, \cdots$的 $n+1$ 次差分等于零,那末 $b_0, b_1, \cdots$ 是一个 n 次多項式 $f(x)$ 的值,这个多項式由公式 (2) 及 (9) 給出.

事实上,若是以多項式 $f(x)$ 的值作一个差分格式并且与上面所給出的格式 (8) 比較,那末就看出,两个格式中各列的第一个元素 $b_0, \Delta b_0, \Delta^2 b_0, \cdots, \Delta^n b_0$ 都一样,而第 $n+1$ 列的元素都是零. 由此依次推出,在两个格式中,第 n 列,第 $n-1$ 列,$\cdots$,最后第一列的元素都相同.

刚才所导出的想法,同时又告訴我們,当各列的第一个元素 $\Delta^k b_0=k!\,\lambda_k(k=0, 1, \cdots, n)$ 給出时,怎样从最后一列开始来計算格式 (8) 中所有的元素. 下面的例子 ($n=3$, $b_0=0$, $\Delta b_0=1$, $\Delta^2 b_0=6$, $\Delta^3 b_0=6$) 可以說明这种計算法:

$$
\begin{array}{ccccccc}
0 & & & & & & \\
 & 1 & & & & & \\
1 & & 6 & & & & \\
 & 7 & & 6 & & & \\
8 & & 12 & & & & \\
 & 19 & & 6 & & & \\
27 & & 18 & & & & \\
 & 37 & & 6 & & & \\
64 & & 24 & & & & \\
 & 61 & & & & & \\
125 & & & & & &
\end{array}
\qquad
\begin{aligned}
\lambda_0 &= 0, \\
\lambda_1 &= 1, \\
\lambda_2 &= \frac{6}{2} = 3, \\
\lambda_3 &= \frac{6}{6} = 1.
\end{aligned}
$$

$$
\begin{aligned}
f(x) &= \lambda_0 + \lambda_1 x + \lambda_2 x(x-1) + \lambda_3 x(x-1)(x-2) \\
&= x + 3x(x-1) + x(x-1)(x-2) = x^3.
\end{aligned}
$$

所謂一个零阶算术数列指的是一个由完全相同的数所組成的数列 $b, b, b, \cdots$，而一个 n 阶算术数列指的是这样的一个数列，它的差分数列是一个 $n-1$ 阶算术数列。很明显，假如格式(8)的第 $n+2$ 列全由零組成，那么它的第一列作成一个 n 阶算术数列。于是，上面的証明也可以如下地叙述：

一个 n **次多項式** $f(x)$ **在点** $0, 1, 2, 3, \cdots$ **的值构成一个** n **阶算术数列，而每一个** n **阶算术数列都是由一个次数最高为** n **的多項式在这些点的值所組成。** 多項式 $f(x)$ 由公式(2)及(9)求得。这样，一个 n 阶算术数列的一般項 b_x 由公式

$$
b_x = f(x) = b_0 + (\Delta b_0)x + \frac{\Delta^2 b_0}{2} x(x-1) + \cdots + \\
+ \frac{\Delta^n b_0}{n!} x(x-1)\cdots(x-n+1)
$$

給出。

差分格式(8)在求由数值表(例如由經驗得出)所給出的函数的插值及积分时可以找到实际应用。設 $b_0, b_1, b_2, \cdots$ 是一个函数 $\varphi(x)$ 对于等距的变量值 $\alpha_0, \alpha_0+h, \alpha_0+2h, \cdots$ 的值，实践表明，对于比較規則的函数以及不太大的步长 h，二次、三次，四次或者

在最复杂的情形五次差分实际上是零，从而这个函数在某些相邻的区間内恰如一个最高是四次的多項式。因此，为了数值內插及积分的目的，可以在表中取 2 至 5 个邻接的值作出一个多項式来代替这个函数. 內插法利用公式(2) 作出；在多数情形，一次及二次差分，从而綫性或二次多項式就够了. 在把差分 $\Delta^k b_\nu$ 换算成差商时，除了因子 $k!$ 外，还有区間长 h 的幂出現；因此代替(9)，我們应用公式

$$\lambda_k = \frac{\Delta^k b_0}{k!\,h^k}.$$

如果变量值 $\alpha_0, \alpha_1, \cdots$ 不是等距的，那末代替差分 $\Delta^k b_\nu$，一开始就应該作出差商(7). 关于計算的詳細情形以及誤差的估計等可参考有关的专著[1].

习题. 1. n 阶算术数列的部分和 $s_m = \sum_{\nu=0}^{m-1} a_\nu$(此处 $s_0 = 0$)构成一个 $n+1$ 阶算术数列。由此导出和的公式

$$s_m = m a_0 + \binom{m}{2} \Delta a_0 + \cdots + \binom{m}{n+1} \Delta^n a_0.$$

2. 給出关于和 $\sum_{\nu=0}^{m-1} \nu$, $\sum_{\nu=0}^{m-1} \nu^2$, $\sum_{\nu=0}^{m-1} \nu^3$ 的公式。

§ 26. 因子分解

在 § 22 里已經看到，对于多項式环 $\mathbf{K}[x]$，此处 $\mathbf{K}$ 是一个域，分解成素因子的唯一分解定理成立. 我們現在将証明以下的更一般的基本定理：

若 $\mathfrak{S}$ 是一个有单位元素的整环，并且在 $\mathfrak{S}$ 中唯一素因子分解定理成立，那末这个定理在多項式环 $\mathfrak{S}[x]$ 中也成立.

---

1) 例如，Kowalewski: Interpolation und genäherte Quadratur, Leipzig, 1930.

这里所举出的証明是属于 Gauss 的。

設 $f(x)=\sum_{0}^{n}a_ix^i$ 是 $\mathfrak{S}[x]$ 中一个异于零的多项式。$a_0,\cdots,a_n$ 在 $\mathfrak{S}$ 中的最大公因子 d（参考 §22，习題 7）叫做 $f(x)$ 的**容度**。把 d 括出，我們有

$$f(x)=d\cdot g(x),$$

其中 $g(x)$ 有容度 1。 $g(x)$ 与 d 除可逆元素的因子外是唯一确定的。具有容度 1 的多項式叫做**本原多項式**(关于 $\mathfrak{S}$ 的)。

引理 1. 两个本原多項式的积仍是一个本原多項式。

証明. 設

$$f(x)=a_0+a_1x+\cdots$$

及

$$g(x)=b_0+b_1x+\cdots$$

是本原多項式。假設 $f(x)\cdot g(x)$ 的系数有一个非可逆元素的最大公因子 d。若 p 是 d 的一个素因子，那末 p 一定能整除 $f(x)g(x)$ 的所有系数。令 a_r 是 $f(x)$ 中第一个不能被 p 整除的系数，b_s 是 $g(x)$ 中第一个不能被 p 整除的系数。

$f(x)g(x)$ 中 x^{r+s} 的系数有形状

$$a_rb_s+a_{r+1}b_{s-1}+a_{r+2}b_{s-2}+\cdots$$
$$+a_{r-1}b_{s+1}+a_{r-2}b_{s+2}+\cdots.$$

这个和应該能被 p 整除。另一方面，除第一項外，其余項都能被 p 整除。因此 a_rb_s 能被 p 整除，于是 a_r 或 b_s 应該能被 p 整除，这与假設相违。

令 Σ 是 $\mathfrak{S}$ 的商域（§16）。于是在 $\Sigma[x]$ 中每一个多項式都能唯一分解(§22)。为了由 $\Sigma[x]$ 中的分解过渡到 $\mathfrak{S}[x]$ 中的一个分解，我們应用以下事实：$\Sigma[x]$ 中每一多項式 $\varphi(x)$ 可以写成 $\frac{F(x)}{b}$ 的形状($F(x)$属于 $\mathfrak{S}[x]$，b 属于 $\mathfrak{S}$)，此处 b 可以看作是 $\varphi(x)$ 中各

个系数分母的积。于是 $F(x)$ 可以写成"容度乘本原多项式"的积：

$$F(x) = af(x),$$

(1) $$\varphi(x) = \frac{a}{b} f(x).$$

我們現在陈述：

引理 2. 在(1)中出現的本原多項式 $f(x)$ 除 $\mathfrak{S}$ 中的可逆元素外由 $\varphi(x)$ 唯一确定。反过来，根据(1)，$\varphi(x)$ 除相差一个 $\Sigma[x]$ 中的可逆元素因子外由 $f(x)$ 唯一确定。按照这种方法，对于 $\Sigma[x]$ 中每一个 $\varphi(x)$ 有一个本原多項式 $f(x)$ 与它对应，那末对于两个多項式的积 $\varphi(x)\cdot\psi(x)$，除可逆元素外，有相应的本原多項式的积与它对应(反过来也对)。若 $\varphi(x)$ 在 $\Sigma[x]$ 中不可分解，那末 $f(x)$ 在 $\mathfrak{S}[x]$ 中也不可分解(反过来也对)。

証明. 設給出 $\varphi(x)$ 的两个不同的表示：

$$\varphi(x) = \frac{a}{b} f(x) = \frac{c}{d} g(x).$$

于是

(2) $$adf(x) = cbg(x).$$

左端的容度是 ad，右端的是 cb；所以必須

$$ad = \varepsilon cb,$$

此处 ε 是 $\mathfrak{S}$ 的一个可逆元素。把这个式子代入(2)并且用 cb 去除，得

$$\varepsilon f(x) = g(x).$$

因此 $f(x)$ 与 $g(x)$ 仅相差 $\mathfrak{S}$ 中的一个可逆元素。

对于两多項式

$$\varphi(x) = \frac{a}{b} f(x),$$

$$\psi(x) = \frac{c}{d} g(x)$$

的积，立刻得

$$\varphi(x)\psi(x)=\frac{ac}{bd}f(x)g(x),$$

根据引理 1，$f(x)g(x)$ 仍是一个本原多項式．因此乘积 $f(x)g(x)$ 与乘积 $\varphi(x)\psi(x)$ 对应．

最后，若 $\varphi(x)$ 不可分解，那末 $f(x)$ 也不可分解；因为由分解 $f(x)=g(x)h(x)$ 将立即导致分解

$$\varphi(x)=\frac{a}{b}f(x)=\frac{a}{b}g(x)\cdot h(x).$$

反过来可以同样証明．

这样，引理 2 被証明．

由引理 2，$\varphi(x)$ 的唯一因子分解可以直接轉到相应的本原多項式上．因此，本原多項式除可逆元素外可以唯一地分解成本原的素因子．

現在轉向 $\mathfrak{S}[x]$ 中任意多項式的因子分解．不可分解的多項式一定或者是一个不可分解的常数，或者是一个不可分解的本原多項式；因为其他每一个多項式总可以分解成容度乘本原多項式．因此要分解一个多項式 $f(x)$，必須首先把 $f(x)$ 分解成容度乘本原多項式，然后再分别将这两部分分解成素因子．前者的分解根据基本定理的假設，除可逆元素外是可能的和唯一的，后者根据方才所証，也是如此．于是基本定理被証明．

作为証明的附带結果，我們有：

若 $\mathfrak{S}[x]$ 中一个多項式 $F(x)$ 在 $\Sigma[x]$ 中可分解，那末它在 $\mathfrak{S}[x]$ 中已經可分解．

因为由 $F(x)=d\cdot f(x)$，有一个本原多項式 $f(x)$ 与 $F(x)$ 对应，并且根据引理 2，$F(x)$ 在 $\Sigma[x]$ 中的一个分解导致 $f(x)$ 在 $\mathfrak{S}[x]$ 中的一个分解；随同 $f(x)$ 一起，$F(x)$ 也可分解．

例如,一个有理整系数多项式若有有理系数分解,那末它也有整系数分解. 因此,当一个整系数多项式不能分解成整系数因子时,它也不能分解成有理系数因子.

利用完全归納法,由基本定理可以得到进一步的結果:

若 $\mathfrak{S}$ 是一个有单位元素的整环并且在 $\mathfrak{S}$ 中唯一因子分解定理成立,那末这个定理在多項式环 $\mathfrak{S}[x_1, \cdots, x_n]$ 中也成立.

由此推出关于整系数多項式(任意个变数的),关于系数取自一个域中的多項式等等的唯一因子分解.

由 Gauss 引理所引入的"本原多項式"的概念,特别在处理多元多項式环时有用. 設 $\mathbf{K}$ 是一个域,$\mathbf{K}[x_1, \cdots, x_n]$ 中多項式 f 說是关于 $x_1, \cdots, x_{n-1}$ 本原的,如果它关于整环 $\mathbf{K}[x_1, \cdots, x_{n-1}]$ 是本原的,换一句話說,它沒有只依賴于 $x_1, \cdots, x_{n-1}$ 的非常数因子.

习題. 1. $\mathfrak{S}[x]$ 中的可逆元素只能是 $\mathfrak{S}$ 中的可逆元素.

2. 証明:在一个齐次多項式的因子分解中,只能有齐次因子出現.

3. 証明:行列式

$$\Delta = \begin{vmatrix} x_{11} \cdots x_{1n} \\ \cdot \quad\quad \cdot \\ \cdot \quad\quad \cdot \\ \cdot \quad\quad \cdot \\ x_{n1} \cdots x_{nn} \end{vmatrix}$$

在多項式环 $\mathfrak{S}[x_{11}, \cdots, x_{nn}]$ 中不可分解.(选取一个不定元,比方說 x_{11},証明 Δ 关于其余不定元是本原的.)

4. 給出一个規則来判定任意一个整系数多項式什么时候有一个一次因子.

5. 証明多項式

$$x^4 - x^2 + 1$$

在关于不定元 x 的整系数多項式环中的不可分解性. 这个多項式在有理系数多項式环中能否分解?它在系数属于 Gauss 环的多項式环中能否分解?

§27. 不可約性判定标准

令 $\mathfrak{S}$ 是一个有单位元素的整环,在其中唯一分解定理成立,又令

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

是 $\mathfrak{S}[x]$ 中一个多項式. 以下定理在多数情形提供一个关于 $f(x)$ 的不可約性的判定.

Eisenstein 定理. 如果在 $\mathfrak{S}$ 中有一素元素 p, 使得

$$a_n \not\equiv 0(p),$$

$$a_i \equiv 0(p) \quad \text{对于} \quad i < n,$$

$$a_0 \not\equiv 0(p^2),$$

那末 $f(x)$ 除常数因子外在 $\mathfrak{S}[x]$ 中不可約; 換一句話說, $f(x)$ 在 $\Sigma[x]$ 中不可約,此处 Σ 是 $\mathfrak{S}$ 的商域.

証明. 假設 $f(x)$ 可分解:

$$f(x) = g(x) \cdot h(x),$$

$$g(x) = \sum_0^r b_\nu x^\nu,$$

$$h(x) = \sum_0^s c_\nu x^\nu,$$

$$r > 0, \quad s > 0, \quad r + s = n,$$

那末

$$a_0 = b_0 c_0 \quad \text{且} \quad a_0 \equiv 0(p).$$

由此推出, 或者 $b_0 \equiv 0(p)$ 或者 $c_0 \equiv 0(p)$. 例如設 $b_0 \equiv 0(p)$, 那末 $c_0 \not\equiv 0(p)$, 否則將有 $a_0 = b_0 c_0 \equiv 0(p^2)$.

不可能 $g(x)$ 的所有系数都能被 p 整除; 因为不然的話, 乘积 $f(x) = g(x)h(x)$ 將能被 p 整除, 从而一切系数,特别 a_n 將能被 p 整除, 这与假定相違. 这样,令 b_i 是 $g(x)$ 中第一个不能被 p 整除的系数 ($0 < i \leqslant r < n$). 那末

$$a_i = b_i c_0 + b_{i-1} c_1 + \cdots + b_0 c_i,$$

$$a_i \equiv 0(p),$$

$$b_{i-1} \equiv 0(p),$$

$$\cdots\cdots\cdots\cdots$$

$$b_0 \equiv 0(p),$$

从而

$$b_i c_0 \equiv 0(p),$$

$$c_0 \not\equiv 0(p),$$

$$b_i \equiv 0(p),$$

与假設矛盾.

因此 $f(x)$ 除常数因子外是不可約的.

例 1. $x^m - p$ (p 是素数) 在整系数(从而在有理系数)多項式环內不可約. 因此 $\sqrt[m]{p}$ ($m > 1$, p 素数)是无理数.

例 2. 当 p 是素数时, $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$ 是"分圓方程"的左端. 我們仍旧問它在整系数(或者,同样地,有理系数)多項式环中是否不可約. Eisenstein 定理不能直接应用;然而可以如下地实現. 假若 $f(x)$ 可約, 那末 $f(x+1)$ 也可約. 我們有

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{x^p + \binom{p}{1} x^{p-1} + \cdots + \binom{p}{p-1} x}{x}$$

$$= x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + \binom{p}{p-1}.$$

除 x^{p-1} 的系数外,一切系数都能被 p 整除;因为在二項式系数公式

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!}$$

中, 对于 $i < p$, 分子能被 p 整除而分母不能被 p 整除. 另一方面, 常数項 $\binom{p}{p-1} = p$ 不能被 p^2 整除. 因此 $f(x+1)$ 不可約,所以 $f(x)$ 不可約.

例 3. 同样的变換也导出关于 $f(x) = x^2 + 1$ 的一个判断,因为

$$f(x+1) = x^2 + 2x + 2.$$

习題. 1. 証明 $\sqrt[m]{p_1 p_2 \cdots p_r}$ 的无理性,此处 $p_1, p_2, \cdots, p_r$ 是互不相同的素数且 $m > 1$.

2. 証明:

$$x^2 + y^2 - 1$$

在 $P[x, y]$ 中的不可約性,此处 P 是任意域,在其中 $+1 \neq -1$.

3. 証明:多項式

$$x^4 + 1; \quad x^6 + x^3 + 1$$

在整系数多項式环中不可約.

从根本上說, Eisenstein 定理是建立在把方程

$$f(x) = g(x) \cdot h(x)$$

变成一个模 p^2 的同余式

$$f(x) \equiv g(x) \cdot h(x),$$

并且由此导出矛盾的基础上的. 在許多其他情形,不可約性的証明也可以这

样导出，即把方程变为以整环 $\mathfrak{S}$ 的某一元素 q 为模的同余式，再来研究所給的多項式 $f(x)$ 对于模 q 是否可分解。特别，若 $\mathfrak{S}$ 是整数环 C，那末在对于 q 的同余类环中只有有限多个具有給定次数的多項式；因此对于模 q 永远只需研究 $f(x)$ 的分解的有限种可能。如果 $f(x)$ 对于模 q 不可約，那末 $f(x)$ 也在 $C[x]$ 中不可約。就是在另外的情形，也有可能由所求对于模 q 的分解引出結論，而这时，在 q 是素数的情形，可以基于多項式对于模 q 的唯一素因子分解定理（§ 22，习题 3）。

例 1. $\mathfrak{S} = C$; $f(x) = x^5 - x^2 + 1$. 若 $f(x)$ 模 2 可分解，那末因子之一必定是綫性的或二次的。現在对于模 2 只有两个綫性多項式：

$$x, \ x+1,$$

并且只有一个二次不可約多項式

$$x^2 + x + 1.$$

施行除法表明，$x^5 - x^2 + 1$ 不能被这些多項式整除（模 2）。这一点可以直接从

$$x^5 - x^2 + 1 = x^2(x^3 - 1) + 1 \equiv x^2(x+1)(x^2+x+1) + 1$$

看出。因此 $f(x)$ 不可約。

例 2. $\mathfrak{S} = C$; $f(x) = x^4 + 3x^3 + 3x^2 - 5$. 对于模 2 分解 $f(x)$：

$$f(x) \equiv (x+1)(x^3+x+1).$$

后一因子对于模 2 不可約。因此，若 $f(x)$ 可分解，那末它必須分解成一个綫性因子及一个三次因子。現在容易直接証明，綫性因子不存在。最方便莫过于这样考慮，即在問題中所出現的对于模 3 仅有的綫性因子 $x, x+1, x-1$ 都不能整除 $f(x)$。

Eisenstein 判定标准的更为广泛的一般化是由 G. Dumas 引出的。令 p 仍是 $\mathfrak{S}$ 中一个素元素。对于 $f(x)$ 每一异于零的項 $ax^\lambda = cp^\mu x^\lambda$，其中 $(c, p) = 1$，有一个指数对 (λ, μ) 属于它。我們可以把这些数对看成 (λ, μ)-平面上格点的坐标，点的个数与 $f(x)$ 的項数相同。

現在对于每一項 $cp^\mu x^\lambda$，給出一个权 $\alpha\lambda + \beta\mu$，此处 α, β 是无公因子的整数并且 $\beta > 0$。这就是說，給予因子 x 以权 α，因子 p 以正权 β，与 p 互素的因子以权 0 并且令乘积的权等于因子的权的和。

在 $f(x)$ 一切項的权中，有一最小值 γ。我們如此选取 α 与 β，使得这个最小值至少取得两次。为此，直綫 $\alpha\lambda + \beta\mu = \gamma$ 应該这样选取，使得所考慮的格点至少有两点在这直綫上并且沒有点在它下面。于是商 $\dfrac{-\alpha}{\beta}$ 作为不可

約分数，是这直綫的斜率。

令 (λ_1, μ_1) 及 (λ_2, μ_2) 是使 $\alpha\lambda + \beta\mu$ 取最小值 γ 的 (λ, μ) 的两对值。选择 λ_1 尽可能地小而 λ_2 尽可能地大。于是由

$$\alpha\lambda_1 + \beta\mu_1 = \alpha\lambda_2 + \beta\mu_2 = \gamma$$

推出

$$\alpha(\lambda_2 - \lambda_1) + \beta(\mu_2 - \mu_1) = 0, \tag{1}$$

因此 $\alpha(\lambda_2 - \lambda_1)$，从而 $\lambda_2 - \lambda_1$ 能被 β 整除：

$$\lambda_2 - \lambda_1 = m\beta, \quad \mu_2 - \mu_1 = -m\alpha, \quad m = (\lambda_2 - \lambda_1, \mu_2 - \mu_1).$$

我們断言：若 $f(x)$ 可分解，那末两个因子多項式的次数必定有以下形式：

$$m_1\beta + r_1 \quad 及 \quad m_2\beta + r_2 \tag{2}$$

$$(m_1, m_2, r_1, r_2 \geqslant 0, \quad m_1 + m_2 = m, \quad r_1 + r_2 = n - m\beta).$$

証明．　設 $f(x) = g_1(x)\cdot g_2(x)$，又令 γ_1 是 $g_1(x)$ 的項的最小权，γ_2 是 $g_2(x)$ 的項的最小权。在 $g_1(x)$ 具有权 γ_1 的各項中令 dx^δ 是有最小指数 δ 的項而 ex^ε 是有最大指数 ε 的項；相应地令 rx^ρ 与 sx^σ 是对于 $g_2(x)$ 所定义的項。当作出乘积 $g_1(x)g_2(x)$ 时，我們得到一些具有权 $\gamma_1 + \gamma_2$ 的項，在其中 $drx^{\delta+\rho}$ 是最小指数項而 $esx^{\varepsilon+\sigma}$ 是最大指数項，至于其他一切項都具較大权．把一个权較大的項加到象 $drx^{\delta+\rho}$ 或 $esx^{\varepsilon+\sigma}$ 那样具有权 $\gamma_1 + \gamma_2$ 的一項上，权不改变。若乘积 g_1g_2 与 $f(x)$ 一致，那末显然必須有

$$\gamma_1 + \gamma_2 = \gamma, \quad \delta + \rho = \lambda_1, \quad \varepsilon + \sigma = \lambda_2.$$

由此推出

$$(\varepsilon - \delta) + (\sigma - \rho) = \lambda_2 - \lambda_1 = m\beta.$$

如同前面 $\lambda_2 - \lambda_1$ 的同样理由，$\varepsilon - \delta$ 及 $\sigma - \rho$ 也必定能被 β 整除，因为 δ 及 ε 对于 $g_1(x)$ 扮演着 λ_1 及 λ_2 对于 $f(x)$ 同样的角色。因此

$$\varepsilon - \delta = m_1\beta, \quad \sigma - \rho = m_2\beta, \quad m_1 + m_2 = m.$$

最后，$g_1(x)$ 的次数至少是 ε，所以 $\geqslant m_1\beta$，同样，$g_2(x)$ 的次数至少是 $m_2\beta$。这样就不难得出上面关于 $g_1(x)$ 与 $g_2(x)$ 的次数的表示式。

推論 1．　(2) 的两个次数中至少有一个 $\geqslant \beta$。

2．若 $f(x)$ 的第一項及最末項有最小权 γ，那末 g_1 与 g_2 的次数可以被 β 整除。

在这一情形有

$$m\beta = \lambda_2 - \lambda_1 = n - 0 = n, \quad r_1 + r_2 = n - m\beta = 0, \quad r_1 = r_2 = 0.$$

3. 若 $\beta = n$，那末 $f(x)$ 不可約(由 1 推出).

特别，取 $\alpha = 1$，$\beta = \gamma = n$，就得到 Eisenstein 判定标准.

例 1. 令 $f(x) = x^n + cp^m$，$(c, p) = 1$，$(m, n) = 1$. 綫性齐式 $m\lambda + n\mu$ 对于 $f(x)$ 的两項的值都是 nm. 因此应該令 $\alpha = m$，$\beta = n$. 由推論 3，$f(x)$ 不可約.

2. 設 $n \geqslant 2$ 而 $f(x) = x^n + px + bp^2$. 綫性齐式 $\lambda + (n-1)\mu$ 对于前两項有值 n，对于最末項有值 $2n - 2 \geqslant n$. 因此可以令 $\alpha = 1$，$\beta = n-1$. 若 $f(x)$ 可分解，那末由 1，因子之一应該有次数 $n - 1$ 从而另一个是綫性的.

§28. 因子分解在有限步下的完成

尽管我們已經看到，对于一个給定的域 Σ，$\Sigma[x_1, \cdots, x_n]$ 中每一多項式在理論上可以分解为素因子，并且在某些情形也給出实际分解的方法或者指出分解的不可能性；然而还缺少一个一般的方法，使得在每一情形經过有限步来完成这种分解. 至少对于 Σ 是有理数域的情形我們給出一个这样的方法.

根据 §26，每一个有理系数多項式总可以假定是整系数的，并且它的分解可以在整系数多項式环中进行. 在整数环 C 本身里，每一素因子分解显然可以通过有限次試驗来实行；此外，又只有有限个可逆元素($+1$ 及 -1)，因此只有有限种可能的分解. 在多項式环 $C[x_1, \cdots, x_n]$ 里可逆元素也只有 $+1$，-1. 通过对于变元的个数 n 作完全归納法，所有这一切可以归結为以下問題：

設在 $\mathfrak{S}$ 中每一因子分解可以在有限步下完成；此外，并設在 $\mathfrak{S}$ 中只有有限个可逆元素. 要求一种方法，把 $\mathfrak{S}[x]$ 中每一多項式分解为素因子.

解是由 Kronecker 給出的.

設 $f(x)$ 是 $\mathfrak{S}[x]$ 中一个 n 次多項式. 若 $f(x)$ 可分解，那末因子之一有次数 $\leqslant \frac{n}{2}$；于是，若 s 是 $\leqslant \frac{n}{2}$ 的最大整数，我們需要研究，$f(x)$ 是否有次数 $\leqslant s$ 的因子.

我們在任意选取的 $s+1$ 个整点 $a_0, a_1, \cdots, a_s$ 上作函数值 $f(a_0)$，$f(a_1)$，$\cdots$，$f(a_s)$. 若 $f(x)$ 可以被 $g(x)$ 整除，那末必須 $f(a_0)$ 能被 $g(a_0)$ 整除，$f(a_1)$ 能被 $g(a_1)$ 整除，等等. 然而因为每一个 $f(a_i)$ 在 $\mathfrak{S}$ 中只有有限多个因子，

因此，对于每一 $g(a_i)$ 只有有限多种可能情形来考察，根据假定，所有这些可能情形都可以找出。对于值 $g(a_0), g(a_1), \cdots, g(a_s)$ 的每一可能組合，根据 § 25 的定理，有且只有一个多項式 $g(x)$ 存在，这个多項式可以（例如，用 Newton 內插公式）明确建立起来。因此作为考察中的因子的多項式 $g(x)$ 只有有限多个。現在应用除法算式就可以断定每一个这样的多項式 $g(x)$ 是否确实是 $f(x)$ 的因子。如果除去可逆元素不計外，这些可能的多項式 $g(x)$ 沒有一个是 $f(x)$ 的因子，那末 $f(x)$ 不可分解；在另外的情形，我們可以求得一个分解并且再对这两个因子应用这种手續，如此等等。

在整系数情形 ($\mathfrak{S} = C$)，这种手續可以大大地簡化。首先，通过所給的多項式对于模 2 或有时对于模 3 的分解，可以得出这样一个梗概，即可能的因子多項式 $g(x)$ 能有怎样的次数以及对于模 2 及模 3，系数属于什么同余类。这就大大地限制了可能的 $g(x)$ 的个数。再者，当应用 Newton 內插公式时，注意到最后系数 λ_s 应該是 $f(x)$ 最高項系数的一个因子，这又意味着可能性的一个限制。最后，利用多于 $s+1$ 个点 a_i 是方便的（最好选取 0，± 1，± 2，…等等）。这样，为了决定可能的 $g(a_i)$，我們用含素因子最少的那些 $f(x)$；其余的点可以在以后用来进一步限制可能性的个数，在其中对于每一个所計算的 $g(x)$，首先試驗它在这些沒有被注意到的点 a_i 上所取的值是不是对应的 $f(a_i)$ 的因子。

习題． 1．在 $C[x]$ 中分解

$$f(x) = x^5 + x^4 + x^2 + x + 2.$$

2．在 $C[x, y, z]$ 中分解

$$f(x, y, z) = -x^3 - y^3 - z^3 + x^2(y+z) + \\ + y^2(x+z) + z^2(x+y) - 2xyz.$$

§ 29. 对称函数

設 $\mathfrak{o}$ 是一个有单位元素的交換环。

$\mathfrak{o}[x_1, \cdots, x_n]$ 中一个多項式，如在不定元 $x_1, \cdots, x_n$ 的任一置换之下都变为自身，就叫做变元 $x_1, \cdots, x_n$ 的一个（有理整的）**对称函数**。例如：变元的和、积、冪和 $s_\rho = \sum_{\nu=1}^{n} x_\nu^\rho$。

引入一个新不定元 z，令

$$
(1) \qquad \begin{cases} f(z) = (z - x_1)(z - x_2)\cdots(z - x_n) \\ \qquad = z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \cdots + (-1)^n \sigma_n, \end{cases}
$$

那末 z 的冪的系数

$$
\begin{cases} \sigma_1 = x_1 + x_2 + \cdots + x_n, \\ \sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_2x_3 + \cdots + x_{n-1}x_n, \\ \sigma_3 = x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \sigma_n = x_1x_2\cdots x_n \end{cases}
$$

显然是对称函数，因为(1)的左端，从而它的右端在 x_i 的一切置換之下都保持不变。我們称 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 为 $x_1, x_2, \cdots, x_n$ 的初等对称函数。

在每一多項式 $\varphi(\sigma_1, \cdots, \sigma_n)$ 中，若把 σ 用它的表达式代入，就产生一个关于 $x_1, \cdots, x_n$ 的对称函数。$\varphi(\sigma_1, \cdots, \sigma_n)$ 的一項 $c\sigma_1^{\mu_1}\cdots\sigma_n^{\mu_n}$ 产生 x_i 的一个次数为 $\mu_1 + 2\mu_2 + \cdots + n\mu_n$ 的齐次对称多項式，因为每一 σ_i 是一个 i 次齐次多項式。我們把和 $\mu_1 + 2\mu_2 + \cdots + n\mu_n$ 叫做項 $c\sigma_1^{\mu_1}\cdots\sigma_n^{\mu_n}$ 的权，而多項式 $\varphi(\sigma_1, \cdots, \sigma_n)$ 的权指的是在它的各項中所出現的最高权。于是，权为 k 的多項式 $\varphi(\sigma_1, \cdots, \sigma_n)$ 产生一个次数 $\leqslant k$ 的对称多項式。

所謂对称函数的基本定理指的是：

$\mathfrak{o}[x_1, \cdots, x_n]$ 中每一个有理整对称函数可以写成多項式 $\varphi(\sigma_1, \cdots, \sigma_n)$。

証明．我們把所給的多項式"字典式地"排列（如同在字典中那样），就是說，一項 $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ 在另一項 $x_1^{\beta_1}\cdots x_n^{\beta_n}$ 的前面，假如第一个非零的差 $\alpha_i - \beta_i$ 是正数。随同一項 $a_1x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ 一起，指数是由 α_i 的一个置換所构成的一切項也都出現；这些項不必全写，只需写作 $a\sum x_1^{\alpha_1}\cdots x_n^{\alpha_n}$，在其中只把和的字典式的首項实际写出。

对于这一項来說，$\alpha_1 \geqslant \alpha_2 \geqslant \cdots \geqslant \alpha_n$ 成立。

設所給的对称多項式次数为 k，字典式的首項是 $ax_1^{\alpha_1}\cdots x_n^{\alpha_n}$。現在做一个初等对称函数的乘积，使它（乘出并且按字典排列时）具有同一首項 $ax_1^{\alpha_1}\cdots x_n^{\alpha_n}$。这一項容易求出，就是

$$a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\cdots\sigma_n^{\alpha_n}.$$

从所給的多項式中減去这一項，再按字典式排列，求首項，如此等等。

这个过程必定在某一步上終結。所指出的乘积自然具有权

$$\alpha_1-\alpha_2+2\alpha_2-2\alpha_3+3\alpha_3-\cdots-(n-1)\alpha_n+n\alpha_n$$
$$=\alpha_1+\alpha_2+\cdots+\alpha_n\leqslant k,$$

因此，当它被写成 x 的多項式时有次数 $\leqslant k$。因此，所給的对称函数的次数通过作減法不会增高。然而对于給定的次数 k，只能有有限多个冪积 $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$。因此，作每一次減法都有这样的一个冪积被消去，并且只剩下較后的字典式排列的項，从而这个过程在有限多步后一定停止，而不再剩下任何項。

这个証明同时提供一个把給定的对称函数通过实际計算用 σ_i 表示的方法。如果我們所給的函数有次数 k，那末所求的表达式 $\varphi(\sigma_1,\cdots,\sigma_n)$ 将有权 k。

由証明中还推出：k 次齐次对称函数可以用 σ_i 的“等权”表达式表出，就是这样的表达式，其中的項都具有同一权 k。

我們現在証明，一个对称函数**只有一种方法**由 $\sigma_1,\cdots,\sigma_n$ 有理整地表示；确切地說：

若 $\varphi_1(y_1,\cdots,y_n)$ **及** $\varphi_2(y_1,\cdots,y_n)$ **是不定元** $y_1,\cdots,y_n$ **的两个多項式且**

$$\varphi_1(y_1,\cdots,y_n)\neq\varphi_2(y_1,\cdots,y_n),$$

那末

$$\varphi_1(\sigma_1,\cdots,\sigma_n)\neq\varphi_2(\sigma_1,\cdots,\sigma_n).$$

作出差 $\varphi_1 - \varphi_2 = \varphi$，我們看出，只需証明：由 $\varphi(y_1, \cdots, y_n) \neq 0$ 可推出 $\varphi(\sigma_1, \cdots, \sigma_n) \neq 0$.

証明. $\varphi(y_1, \cdots, y_n)$ 中每一項可以写成

$$a y_1^{\alpha_1-\alpha_2} y_2^{\alpha_2-\alpha_3} \cdots y_n^{\alpha_n}$$

的形式. 在一切属于系数 $a \neq 0$ 的組 $(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 中，有一个字典式的首項. 以 σ_i 代替 y_i，并且把它用 x_i 表出，那末作为 $\varphi(\sigma_1, \cdots, \sigma_n)$ 中字典式的首項，我們得到

$$a x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

这一項不能被消去，因此确实 $\varphi(\sigma_1, \cdots, \sigma_n) \neq 0$.

这样就証明了：

$\mathfrak{o}[x_1, \cdots, x_n]$ 中每一对称多項式可以用一种而且仅一种方法写成 $\sigma_1, \cdots, \sigma_n$ 的多項式；这个多項式的权等于所給的多項式的次数.

当 x_i 不是不定元，而是 $\mathfrak{o}$ 中的量，例如，是一个在 $\mathfrak{o}[z]$ 中完全分解的多項式 $f(z)$ 的根时，对称函数間的有理整关系仍旧保持成立. 因此，由所証明的事实得出，$f(z)$ 的根的每一对称函数可以用 $f(z)$ 的系数表示.

习題. 1. 对于任意 n，将“冪和” Σx_1, Σx_1^2, Σx_1^3 用初等对称函数表出。

2. 設 $\Sigma x_1^\rho = s_\rho$. 証明公式

$$s_\rho - s_{\rho-1}\sigma_1 + s_{\rho-2}\sigma_2 - \cdots + (-1)^{\rho-1} s_1 \sigma_{\rho-1} + (-1)^\rho \rho \sigma_\rho = 0, \quad \text{对于 } \rho \leq n,$$

$$s_\rho - s_{\rho-1}\sigma_1 + \cdots + (-1)^n s_{\rho-n}\sigma_n = 0, \quad \text{对于 } \rho > n,$$

并且利用这些公式，将冪和 s_1, s_2, s_3, s_4, s_5 用初等对称函数表出。

3. 根据基本定理，令

$$s_\rho = \Sigma a_{\lambda_1, \cdots, \lambda_n} \sigma_1^{\lambda_1} \cdots \sigma_n^{\lambda_n}$$

(对一切 λ_i 求和，其中 $\lambda_1 + 2\lambda_2 + 3\lambda_3 + \cdots = \rho$)，于是由习題 2 得出一个关于 $a_{\lambda_1 \cdots \lambda_n}$ 的遞推公式：

$$a_{\lambda_1, \cdots, \lambda_n} = a_{\lambda_1 - 1, \cdots, \lambda_n} - a_{\lambda_1, \lambda_2 - 1, \cdots, \lambda_n} + \cdots [+ (-1)^{\rho-1}\rho],$$

此处在方括号内的項仅当 $\lambda_\rho = 1$ 而其余 $\lambda_i = 0$ 时才出現(而且作为单独一項出現)，并且令一切具有負下标的 a 等于零。 証明，这个递推关系式的解是：

$$a_{\lambda_1, \cdots, \lambda_n} = (-1)^{\lambda_2+\lambda_4+\lambda_6+\cdots} \frac{\rho \cdot (\lambda_1 + \lambda_2 + \cdots + \lambda_n - 1)!}{\lambda_1! \lambda_2! \cdots \lambda_n!}.$$

一个重要的对称多項式就是差积的平方：

$$D = \prod_{i<k} (x_i - x_k)^2.$$

表达式 D 作为 $a_1 = -\sigma_1, a_2 = \sigma_2, \cdots, a_n = (-1)^n \sigma_n$ 的多項式，叫做多項式 $f(z) = z^n + a_1 z^{n-1} + \cdots + a_n$ 的**判别式**；对于特殊的 $a_1, \cdots, a_n$，判别式等于零表示 $f(z)$ 有一个重綫性因子。

一般，令多項式 $f(z)$ 带有一个首系数 a_0：

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n,$$

那末

$$\sigma_1 = -\frac{a_1}{a_0}, \sigma_2 = \frac{a_2}{a_0}, \cdots, \sigma_n = (-1)^n \frac{a_n}{a_0}.$$

在这一情形，我們把差积乘以 a_0^{2n-2} 作为判别式：

$$D = a_0^{2n-2} \prod_{i<k} (x_i - x_k)^2.$$

在 § 31 我們将看到，D 是 $a_0, a_1, \cdots, a_n$ 的一个多項式。

应用上述的一般方法，我們求得 $a_0 x^2 + a_1 x + a_2$ 的判别式是：

$$D = a_1^2 - 4a_0 a_2,$$

$a_0 x^3 + a_1 x^2 + a_2 x + a_3$ 的判别式是：

$$D = a_1^2 a_2^2 - 4a_0 a_2^3 - 4a_1^3 a_3 - 27a_0^2 a_3^2 + 18a_0 a_1 a_2 a_3.$$

习题． 4． 将一切 x_i 用 $x_i + h$ 代替，判别式保持不变。由此导出微分条件：

$$na_0 \frac{\partial D}{\partial a_1} + (n-1) a_1 \frac{\partial D}{\partial a_2} + \cdots + a_{n-1} \frac{\partial D}{\partial a_n} = 0.$$

§30. 两个多項式的結式

設 $\mathbf{K}$ 是一个任意域，又設

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n,$$
$$g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m$$

是 $\mathbf{K}[x]$ 中两个多項式. 我們希望寻求这两个多項式有一个非常数公因子 $\varphi(x)$ 的必要且充分的条件.

我們一开始就不把 $a_0 = 0$ 或 $b_0 = 0$ 这种可能性除外，从而实际上 $f(x)$ 的次数可能小于 n 或 $g(x)$ 的次数小于 m. 当多項式 $f(x)$ 被写成上面的形式，即从項 a_0x^n（有时是零）开始时，那末就称 n 为这个多項式的形式次数而称 a_0 为形式首項系数. 我們暂且假定，两个首項系数 a_0, b_0 中至少有一个不为零.

在这个假定下，我們首先証明：$f(x)$ 与 $g(x)$ 有一个非常数公因子，当且仅当有一个形式如

$$h(x)f(x) = k(x)g(x) \tag{1}$$

的方程成立，此处 $h(x)$ 最高是 $m-1$ 次，$k(x)$ 最高是 $n-1$ 次并且两多項式 h, k 不同时恆等于零.

若 (1) 被满足，我們把方程 (1) 的两端分解成素因子，那末左右两端所出現的必定相同. 我們可以假定，例如，$f(x)$ 确实有次数 $n(a_0 \neq 0)$；因为不然的話只需交換 $f(x)$ 与 $g(x)$ 所处的地位就可以了. $f(x)$ 的一切素因子必定在 (1) 式右端同在 $f(x)$ 中出現一样多次，然而不能全部出現在 $k(x)$ 內；因为 $k(x)$ 的次数最高是 $n-1$. 因此有 $f(x)$ 的一个素因子也在 $g(x)$ 中出現. 这就是所要証明的.

反过来，若 $\varphi(x)$ 是 $f(x)$ 与 $g(x)$ 的一个非常数公因子，那末只要令

$$f(x) = \varphi(x)k(x),$$
$$g(x) = \varphi(x)h(x),$$

方程(1)即被满足。

为了进一步研究方程(1)，我們令

$$h(x) = c_0x^{m-1} + c_1x^{m-2} + \cdots + c_{m-1},$$
$$k(x) = d_0x^{n-1} + d_1x^{n-2} + \cdots + d_{n-1}.$$

算出方程(1)并且比較左右两端的冪 $x^{n+m-1}, x^{n+m-2}, \cdots, x, 1$ 的系数，我們得到下面关于系数 c_i 与 d_j 的綫性方程組：

$$(2)\quad \begin{cases} c_0a_0 = d_0b_0, \\ c_0a_1 + c_1a_0 = d_0b_1 + d_1b_0, \\ c_0a_2 + c_1a_1 + c_2a_0 = d_0b_2 + d_1b_1 + d_2b_0, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ c_{m-2}a_n + c_{m-1}a_{n-1} = d_{n-2}b_m + d_{n-1}b_{m-1}, \\ c_{m-1}a_n = d_{n-1}b_m. \end{cases}$$

这是关于 $n+m$ 个量 c_i, d_j 的 $n+m$ 个方程的綫性方程組。希望这些元素不全为零，这个条件就是行列式等于零。为了避免行列式中的減号，把(2)式右端移到左端，我們可以把 c_i 与 $-d_j$ 看作未知量。交換行列式的行与列(对于主对角綫作鏡面反射)，这个行列式取以下形式

$$(3)\qquad R = \begin{vmatrix} a_0a_1\cdots a_n & & & \\ & a_0a_1\cdots a_n & & \\ & & \cdots\cdots\cdots & \\ & & & a_0a_1\cdots a_n \\ b_0b_1\cdots b_m & & & \\ & b_0b_1\cdots b_m & & \\ & & \cdots\cdots\cdots & \\ & & & b_0b_1\cdots b_m \end{vmatrix}.$$

（在沒有写的地方都認为是零。）

上面所写出的行列式叫做多項式 $f(x)$ 与 $g(x)$ 的**結式**。要注意这个行列式是关于 a_i 的 m 次齐式以及关于 b_j 的 n 次齐式；再者，它含有“主項” $a_0^m b_m^n$（主对角綫），最后，它不仅当 f, g 有一个公因子时等于零，而且当（与开始的假定相反）$a_0 = b_0 = 0$ 时也等于零。

我們总結如下：

两个多項式 $f(x)$, $g(x)$ 的結式是它們的系数的形式如（3）的有理整式。若結式等于零，那末多項式 f, g 或者有一非常数公因子，或者它們的首項系数都是零。反过来也成立。

在这里所依据的消去法起源于 Euler；結式的形式（3）多半以 Sylvester 命名。

在定理陈述中的例外情形 $a_0 = b_0 = 0$ 可以如此避免，取两个二元齐式：

$$F(x) = a_0x_1^n + a_1x_1^{n-1}x_2 + \cdots + a_nx_2^n,$$

$$G(x) = b_0x_1^m + b_1x_1^{m-1}x_2 + \cdots + b_mx_2^m$$

代替两个一元多項式。原来的多項式 f, g 以及数 m, n 唯一确定齐式 F, G；反过来也对。f 的每一分解：

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$$

$$= (p_0x^r + \cdots + p_r)(q_0x^s + \cdots + q_s)$$

对应于 F 的一个分解：

$$F(x) = a_0x_1^n + a_1x_1^{n-1}x_2 + \cdots + a_nx_2^n$$

$$= (p_0x_1^r + \cdots + p_rx_2^r)(q_0x_1^s + \cdots + q_sx_2^s),$$

相应地对 g 与 G 也成立。因此，对于 f 与 g 的每一公因子，有 F 与 G 的一个公因子与它对应。反过来，F 或 G 的每一分解，在其中令 $x_1 = x$, $x_2 = 1$，就分別产生 f 或 g 的一个分解，而 F 与 G 的每一

公因子产生 f 与 g 的一个公因子；然而可能 F 与 G 的公因子是 x_2 的一个純冪，从而 f 与 g 对应的公因子是一个常数．但是在 F 与 G 都能被 x_2 整除的情形正是 $a_0=b_0=0$ 的情形；因此在上面定理中所陈述的結式等于零的两种情形可以归并为单一的叙述：F 与 G 有一个非常数的齐次公因子．

我們导入一个重要的恆等式．現在設多項式 $f(x)$，$g(x)$ 的系数 a_μ，b_ν 是不定元．我們作

$$
\begin{aligned}
x^{m-1}f(x) &= a_0x^{n+m-1}+a_1x^{n+m-2}+\cdots+a_nx^{m-1},\\
x^{m-2}f(x) &= \qquad a_0x^{n+m-2}+\cdots\qquad+a_nx^{m-2},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
f(x) &= \qquad\qquad a_0x^n+\cdots\qquad+a_n,\\
x^{n-1}g(x) &= b_0x^{n+m-1}+b_1x^{n+m-2}+\cdots+b_mx^{n-1},\\
x^{n-2}g(x) &= \qquad b_0x^{n+m-2}+\cdots\qquad+b_mx^{n-2},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
g(x) &= \qquad\qquad b_0x^m+\cdots\qquad+b_m.
\end{aligned}
$$

这个方程組的行列式正是 R．若是用最后一列的代数余子式去乘并且相加，消去右端的 x^{n+m-1}，$\cdots$，x，那末就得到一个形式如

$$
Af+Bg=R \tag{4}
$$

的恆等式[1]，其中 A 与 B 是不定元 a_μ，b_ν，x 的整系数多項式．

习題． 1．給出一个关于 $f(x)$ 与 $g(x)$ 有一个至少 k 次公因子的行列式判定标准．

2．对于两个二次多項式来說，

$$
4R=(2a_0b_2-a_1b_1+2a_2b_0)^2-(4a_0a_2-a_1^2)(4b_0b_2-b_1^2).
$$

§31．結式作为根的对称函数

我們現在假設多項式 $f(x)$ 与 $g(x)$ 完全分解成綫性因子：

1）对于齐式 F 与 G，对应的关系是：

$$
AF+BG=x_2^{n+m-1}R.
$$

$$f(x) = a_0(x - x_1)(x - x_2)\cdots(x - x_n),$$
$$g(x) = b_0(x - y_1)(x - y_2)\cdots(x - y_m).$$

$f(x)$ 的系数 a_μ 是 a_0 与根 $x_1, \cdots, x_n$ 的初等对称函数的乘积，同样，b_ν 是 b_0 与 y_k 的初等对称函数的乘积．結式 R 是 a_μ 的 m 次齐式又是 b_ν 的 n 次齐式；因此 R 等于 x_i 与 y_k 的一个对称函数乘以 $a_0^m b_0^n$．

現在首先假定根 x_i 与 y_k 是不定元．多項式 R 在 $x_i = y_k$ 时变成零，因为在这一情形多項式 $f(x)$ 与 $g(x)$ 有一个綫性公因子．因此 R 可以被 $x_i - y_k$ 整除(§ 24)．由于綫性因子 $x_i - y_k$ 彼此无公因子，R 必須能被乘积

$$(1) \qquad S = a_0^m b_0^n \prod_i \prod_k (x_i - y_k)$$

整除．現在这个乘积可以通过两种方式改写．首先，由

$$g(x) = b_0 \prod_k (x - y_k),$$

以 $x = x_i$ 代入并且作乘积

$$\prod_i g(x_i) = b_0^n \prod_i \prod_k (x_i - y_k),$$

从而

$$(2) \qquad S = a_0^m \prod_i g(x_i).$$

其次，按同样方法，由

$$f(x) = a_0 \prod_i (x - x_i) = (-1)^n a_0 \prod_i (x_i - x)$$

得出

$$(3) \qquad S = (-1)^{nm} b_0^n \prod_k f(y_k).$$

由(2)看出，S 是关于 b 的 n 次齐次整式，由(3)，S 是关于 a

的 n 次齐次整式。 但 R 与 S 有同一次数并且可以被 S 整除；从而 R 除去一个常数因子外由 S 唯一确定。比較含 b_m 的最高冪的項，在 R 和 S 中得出同一項 $+ a_0^m b_m^n$；所以这个常数因子有值 1 而

$$R = S.$$

这样，我們求出 R 的三种表示 (1), (2), (3)。根据 § 29 中唯一性定理，(2) 对于 b_ν 以及 (3) 对于 a_μ 恆等地成立；这就是説，(2) 在 $g(x)$ 沒有分解成綫性因子时也成立，而 (3) 在 $f(x)$ 沒有分解成綫性因子时也成立。

由此也容易得出，作为不定元 $a_0, \cdots, b_m$ 的多項式，結式的不可分解性，不仅在整系数多項式环中不可分解，而且是絕对不可約的，就是説，在这些不定元以任意域作为系数域的多項式环中也不可分解。因为如果 R 可以分解成两个因子 A, B，那末也可以把 A 与 B 写成根的对称函数。 由于 R 能被 $x_1 - y_1$ 整除，所以 A 或 B，例如 A 也可以被 $x_1 - y_1$ 整除。于是作为对称函数，A 又必須能被一切其他的 $x_i - y_k$ 整除，因而能被它們的积

$$\prod_i \prod_k (x_i - y_k)$$

整除。因为

$$R = a_0^m b_0^n \prod_i \prod_k (x_i - y_k),$$

所以对于另一因子 B 只剩下可能性 $B = a_0^p b_0^q$。 然而 R 作为 a 与 b 的多項式，既不能被 a_0 也不能被 b_0 整除；因此只剩下 $B = 1$。这就証明了 R 的不可約性。

另一証明可以在 F. S. Macaulay: Algebraic Theory of Modular Systems, § 3, Cambridge, 1961 中找到。

在两个多項式的結式及一个多項式的判别式之間存在一个有趣的关系。由多項式

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n=$$
$$=a_0(x-x_1)(x-x_2)\cdots(x-x_n)$$

与它的导数 $f'(x)$ 作結式 $R(f,f')$，那末由（2）得

$$R(f,f')=a_0^{n-1}\prod_i f'(x_i). \tag{4}$$

根据乘积的微分规則，我們有

$$f'(x)=\sum_i a_0(x-x_1)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_n),$$

$$f'(x_i)=a_0(x_i-x_1)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_n).$$

把它代入（4），我們得到

$$R(f,f')=a_0^{2n-1}\prod_{i\neq k}(x_i-x_k),$$

或者，当 D 表示判别式时，

$$R(f,f')=\pm a_0D. \tag{5}$$

按 § 30 把 $R(f,f')$ 写成行列式，那末可以由第一列提出因子 a_0；因此 D 是 $a_0,\cdots,a_n$ 的一个多項式。再者，（5）自然对于 $a_0,\cdots,a_n$ 恆等地成立而与 $f(x)$ 实际上能否分解成綫性因子无关。

习題. 1. f 与 g 的結式对于系数 a 与 b 一起来說是等权的，它的权是 mn（参考 § 29）。

2. 若 $y_1,\cdots,y_{n-1}$ 是 $f'(x)$ 的零点，那末

$$D=n^n a_0^{n-1}\prod_k f(y_k).$$

3. 判别式 D 等于零，当且仅当 $f(x)$ 与 $f'(x)$ 有一个公因子。若是这一情形，那末在 $f(x)$ 的素因子分解中或者有一个重因子出現，或者有这样的一个因子，它的导数恆等于零。

§ 32. 有理函数的部分分式分解

下面关于有理整函数的定理是有理函数部分分式分解的依据：若 $g(x)$ 与 $h(x)$ 是域 K 上两个无公因子的多項式，a 是 $g(x)$

的次数，b 是 $h(x)$ 的次数而 $f(x)$ 是任意一个次数小于 $a+b$ 的多項式，那末恆等式

$$(1)\qquad f(x)=r(x)g(x)+s(x)h(x)$$

成立，其中 $r(x)$ 有次数 $<b$ 而 $s(x)$ 有次数 $<a$.

証明. 根据假設，$g(x)$ 与 $h(x)$ 的最大公因子等于1，因此恆等式

$$1=c(x)g(x)+d(x)h(x)$$

成立. 用 $f(x)$ 乘这个恆等式，我們得到

$$(2)\qquad f(x)=f(x)c(x)g(x)+f(x)d(x)h(x).$$

为了使 $f(x)c(x)$ 的次数 $<b$，我們用 $h(x)$ 除这个多項式：

$$(3)\qquad f(x)c(x)=q(x)h(x)+r(x),$$

此处 $r(x)$ 的次数小于 $h(x)$ 的次数因而小于 b. 把 (3) 代入 (2)，由此得出

$$f(x)=r(x)g(x)+\{f(x)d(x)+q(x)g(x)\}h(x)=$$
$$=r(x)g(x)+s(x)h(x).$$

其中左端与右端第一項有次数 $<a+b$，所以右項最末一項也应該有次数 $<a+b$，从而 $s(x)$ 的次数小于 a. 这样，上面的定理被証明.

如果把恆等式 (1) 的两端都除以 $g(x)h(x)$，那末就得到分式 $\dfrac{f(x)}{g(x)h(x)}$ 被分成两个部分分式的分解：

$$\frac{f(x)}{g(x)h(x)}=\frac{r(x)}{h(x)}+\frac{s(x)}{g(x)}.$$

根据假定，左端分子的次数小于分母的次数. 对于右端两个部分分式来說情形一样. 如果这些分式之一的分母还能再分解为两个无公因子的因子，那末这个分式又能分解成两个部分分式. 因此可以継續进行，直到分母变成素多項式的冪时为止. 由于这个方

法，就得到如下表述的部分分式分解定理：

每一个分子次数小于分母次数的分式 $f(x)/k(x)$ 可以表示成部分分式的和，这样的部分分式的分母是分母 $k(x)$ 所分解成的素多項式的冪。

这样所得到的具有分母 $q(x)=p(x)^t$ 的部分分式 $r(x)/q(x)$ 还可以进一步分解。設素多項式 $p(x)$ 有次数 l，那末 $q(x)$ 有次数 lt。于是可以先用 $p(x)^{t-1}$ 去除次数 $< lt$ 的分子 $r(x)$ 而带有一个次数 $< l(t-1)$ 的余項，然后再用 $p(x)^{t-2}$ 除这个余項而带有一个次数 $< l(t-2)$ 的余項，如此等等：

$$r(x)=s_1(x)p(x)^{t-1}+r_1(x),$$
$$r_1(x)=s_2(x)p(x)^{t-2}+r_2(x),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$r_{t-2}(x)=s_{t-1}(x)p(x)+r_{t-1}(x),$$
$$r_{t-1}(x)=s_t(x).$$

商 $s_1,\cdots,s_t$ 的次数都 $< l$。由所有这些方程一起推出

$$r(x)=s_1(x)p(x)^{t-1}+s_2(x)p(x)^{t-2}+\cdots+s_{t-1}(x)p(x)+s_t(x),$$
$$\frac{r(x)}{p(x)^t}=\frac{s_1(x)}{p(x)}+\frac{s_2(x)}{p(x)^2}+\cdots+\frac{s_{t-1}(x)}{p(x)^{t-1}}+\frac{s_t(x)}{p(x)^t}.$$

于是得到部分分式分解定理的第二表述：

每一个分子的次数小于分母的次数且分母有素因子分解

$$k(x)=p_1(x)^{t_1}p_2(x)^{t_2}\cdots p_h(x)^{t_h}$$

的分式 $f(x)/k(x)$ 是部分分式的和，部分分式的分母是冪 $p_\nu(x)^{\mu_\nu}$ ($\mu_\nu=1,2,\cdots,t_\nu$; $\nu=1,2,\cdots,h$) 而分子或者是零，或者有一个較分母中素多項式 $p_\nu(x)$ 的次数小的次数。

特别，若素因子 $p_\nu(x)$ 都是綫性的，那末部分分式的分子是常数。在这一重要的特殊情形中，部分分式分解可以按一个非常簡

单的方法作出，就是逐次分解出分母具有最高可能幂指数的部分分式，从而分母的次数逐渐降低。如果我們把分母写成 $k(x) = (x-a)^t g(x)$ 的形式，此处 $g(x)$ 不再含有因子 $x-a$，那末就有

$$(5) \qquad \frac{f(x)}{k(x)} = \frac{f(x)}{(x-a)^t g(x)} = \frac{b}{(x-a)^t} + \frac{f(x)-bg(x)}{(x-a)^t g(x)},$$

其中常数 b 常常可以这样确定，使得第二个分式的分子对于 $x=a$ 等于零从而可以被 $x-a$ 整除：

$$f(a) - bg(a) = 0,$$

$$f(x) - b\cdot g(x) = (x-a)f_1(x).$$

現在可以在(5)式第二个分式中約去因子 $x-a$，然后再对这个分式用同样方法处理，直到完全分解成部分分式时为止。

第五章　域　論

这一章的目的是給出关于域的构造以及它們的最簡单的子域及扩域的一个初步概要。同时下面的某些討論（§§ 33,34,36,37）对于体来說也成立。

§ 33. 子体。素体

令 Σ 是一个体。

当 Σ 的一个子集 Δ 也是一个体时，就称它是 Σ 的一个子体。对此必要且充分的是，Δ 首先是一个子环（即随同 a 与 b 一起，也含有 $a-b$ 及 $a\cdot b$），其次，它含有单位元素并且对于每一 $a\neq 0$，也含有逆元 a^{-1}。代替这个条件，我們也可以要求，Δ 含有一个非零元素并且随同 a 与 b 一起也含有 $a-b$ 及 ab^{-1}。

显然有：

Σ 的任意多个子体的交仍是 Σ 的一个子体。

一个素体是一个不含真子体的体。以下将看到，一切素体都是交换的。

在每一体 Σ 中存在而且只存在一个素体。

証明。 Σ 的一切子体的交是一个体，它显然不再含有真子体。

假定存在两个不同的素体，那末它們的交将是这两个体的子体，从而与这两个体恆等；于是这两个体不能互异。

素体的类型。 設 Π 是包含在 Σ 內的素体。它含有零元素与

单位元素 e，从而也含有一切整数倍 $n \cdot e = \pm \Sigma e$。

这样的元素 ne 的加法与乘法按以下规则施行：

$$ne + me = (n+m)e,$$

$$ne \cdot me = nm \cdot e^2 = nm \cdot e.$$

这样，整数倍 ne 組成一个交換环 $\mathfrak{P}$。再者，通过 $n \to ne$ 給出整数环 C 到环 $\mathfrak{P}$ 上的一个同态映射。于是根据同态定理（§ 19），$\mathfrak{P}$ 与同余类环 $C/\mathfrak{p}$ 同构，此处 $\mathfrak{p}$ 是零所对应的整数 n 所組成的理想，因此对于这样的 n 有 $ne = 0$。

由于 $\mathfrak{P}$ 不含有零因子，所以 $C/\mathfrak{p}$ 也不能含有零因子；从而 $\mathfrak{p}$ 一定是一个素理想。再者，$\mathfrak{p}$ 不可能是单位理想，因为不然的話将有 $1 \cdot e = 0$。于是有两种可能：

1. $\mathfrak{p} = (p)$，此处 p 是一个素数。于是 p 是具有性質 $pe = 0$ 的最小正数。由此推出

$$\mathfrak{P} \cong C/(p).$$

$C/(p)$ 是一个域；所以环 $\mathfrak{P}$ 也是一个域，因而就是所求的素体。于是，在这一情形，素体 Π 与整数环关于一个素数的同余类环同构：元素 $n \cdot e$ 的运算与数 $n \bmod p$ 的同余类的运算一样。

2. $\mathfrak{p} = (0)$。同态 $C \to \mathfrak{P}$ 是一个同构。这时倍数 ne 都不相同：由 $ne = 0$ 推出 $n = 0$。在这一情形环 $\mathfrak{P}$ 还不是域；因为整数环不是域。素体 Π 不仅含有 $\mathfrak{P}$ 的元素，而且还必須含有这些元素的商。由 § 16 知道，同构的整环 $\mathfrak{P}$，C 也一定有同构的商域，从而在这一情形，素体 Π 与有理数域 Γ 同构。

因此，一般来說，包含在 Σ 內的素体的构造由生成理想 $\mathfrak{p}$ 的数 p 或 0 完全决定。正如上面所說的那样，$\mathfrak{p}$ 由具有性質 $ne = 0$ 的数 n 所組成。数 p 或 0 叫做体 Σ 或素体 Π 的特征。

通常的数域或包含有理数域的函数域具有特征零。

由特征的定义立刻得出以下定理：

設 $a \neq 0$ 是 Σ 的一个元素，而 k 是 Σ 的特征．那末由 $na = ma$ 推出 $n \equiv m(k)$．反过来也对．

証明．　用 a^{-1} 乘等式 $na = ma$ 得 $ne = me$，从而根据特征的定义，$n \equiv m(k)$．这个論断是可逆的．

同样可証，由 $na = nb$ 且 $n \not\equiv 0(k)$ 推出 $a = b$．

我們再导出一个重要的运算规则：

在特征 p 的域里

$$(a+b)^p = a^p + b^p,$$
$$(a-b)^p = a^p - b^p.$$

証明．　二項式定理

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + b^p$$

成立（§14，問題5）．然而对于 $0 < i < p$：

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1\cdot 2\cdots i} \equiv 0(p),$$

因为分子含有因子 p 不能被約去．所以只剩下項 a^p 及 b^p：

$$(a+b)^p = a^p + b^p.$$

以 $a + b = a'$ 代入，于是得

$$a'^p = (a'-b)^p + b^p,$$
$$(a'-b)^p = a'^p - b^p,$$

两个論断都被証明．

习題．　1．通过对 f 作归納法証明，对于特征 p：

$$(a+b)^{p^f} = a^{p^f} + b^{p^f},$$
$$(a-b)^{p^f} = a^{p^f} - b^{p^f}.$$

2．同样：

$$(a_1 + a_2 + \cdots + a_n)^p = a_1^p + a_2^p + \cdots + a_n^p.$$

3．应用习題2到和 $1 + 1 + \cdots + 1$ 模 p 上．

4. 证明：对于特征 p,

$$(a-b)^{p-1}=\sum_{j=0}^{p-1}a^jb^{p-1-j}.$$

5. 在 Gauss 整数环（§ 20，习题 3）中，素理想 $(1+i)$，(3)，$(2+i)$ 的同余类环的特征是什么？

§ 34. 添　　加

如果 Δ 是体 Σ 的一个子体，那末就說，Ω 是 Δ 的一个**扩体**或**包括体**. 我們的目的是要得出关于一个給定体的一切可能扩体的一个概貌. 这样同时也就得出关于一切可能体的一个概貌，因为每一个体总可以看成它所包含的素体的扩体. 然而这个目的只在交换的情形对于其中最重要的部分被認为已經达到.

首先設 Ω 是 Δ 的任意一个扩体，而 $\mathfrak{S}$ 是 Ω 中元素的一个任意集. 存在一个包有 Δ 及 $\mathfrak{S}$ 的体；因为 Ω 就是这样的一个. 一切包有 Δ 及 $\mathfrak{S}$ 的体的交本身是一个体，它包有 Δ 及 $\mathfrak{S}$，并且記作 $\Delta(\mathfrak{S})$. 它是包有 Δ 及 $\mathfrak{S}$ 的最小体. 我們說，$\Delta(\mathfrak{S})$ 由 Δ 通过**添加**(体添加)集 $\mathfrak{S}$ 而生成的. 我們有

$$\Delta\subseteq\Delta(\mathfrak{S})\subseteq\Omega,$$

并且两个极端情形是：$\Delta(\mathfrak{S})=\Delta$，$\Delta(\mathfrak{S})=\Omega$.

Δ 的一切元素以及 $\mathfrak{S}$ 的一切元素都属于 $\Delta(\mathfrak{S})$，从而一切由 Δ 及 $\mathfrak{S}$ 的元素通过加，減，乘，除所生成的元素也属于 $\Delta(\mathfrak{S})$. 这些元素的全体已經作成一个体，从而它必須恆等于 $\Delta(\mathfrak{S})$. 于是：$\Delta(\mathfrak{S})$ **是由** $\mathfrak{S}$ **的元素与** Δ **的元素的一切有理組合所构成的**. 在交換的情形这种組合可以簡单地写成 $\mathfrak{S}$ 的元素的有理整函数的商，系数取自 Δ.

若 $\mathfrak{S}$ 是一个有限集：$\mathfrak{S}=\{u_1,\cdots,u_n\}$，那末也可以把 $\Delta(\mathfrak{S})$ 写作 $\Delta(u_1,\cdots,u_n)$. 这时也說添加元素 $u_1,\cdots,u_n$ 于 Δ. 因此，

圓括号永远表示体添加，同时方括号，例如，$\Delta[x]$，表示环添加（一切有理整的組合）.

在 $\Delta(\mathfrak{S})$ 的元素由 Δ 及 $\mathfrak{S}$ 的元素的有理表达式里，任何时候只有 $\mathfrak{S}$ 的有限多个元素出現. 因此，体 $\Delta(\mathfrak{S})$ 的每一元素已經属于一个体 $\Delta(\mathfrak{T})$，此处 $\mathfrak{T}$ 是 $\mathfrak{S}$ 的一个有限子集. 因此，$\Delta(\mathfrak{S})$ 是一切体 $\Delta(\mathfrak{T})$ 的并，此处 $\mathfrak{T}$ 永远是 $\mathfrak{S}$ 的一个有限子集. 这样，添加一个任意集就归結为添加有限集并且作一个并集.

若 $\mathfrak{S}$ 是 $\mathfrak{S}_1$ 与 $\mathfrak{S}_2$ 的并，那末显然

$$\Delta(\mathfrak{S}) = \Delta(\mathfrak{S}_1)(\mathfrak{S}_2).$$

因为 $\Delta(\mathfrak{S}_1)(\mathfrak{S}_2)$ 包含 $\Delta(\mathfrak{S}_1)$ 及 $\mathfrak{S}_2$，从而包含 Δ，$\mathfrak{S}_1$ 及 $\mathfrak{S}_2$，即包含 Δ 及 $\mathfrak{S}$，反过来，$\Delta(\mathfrak{S})$ 包含 Δ，$\mathfrak{S}_1$ 及 $\mathfrak{S}_2$，因而包含 $\Delta(\mathfrak{S}_1)$ 及 $\mathfrak{S}_2$，即包含 $\Delta(\mathfrak{S}_1)(\mathfrak{S}_2)$.

这样，添加一个有限集就归結为有限回依次添加一个单独元素. 通过添加一个单独元素的扩张叫做**单純体扩张**. 我們将在下一节来研究它.

§ 35. 单純域扩张

整个这一节里所研究的都是域. 仍旧設 $\Delta \subseteq \Omega$，而 ϑ 是 Ω 中一个任意元素；我們来研究单純扩域 $\Delta(\vartheta)$.

这个域首先包含一切多項式 $\sum a_k\vartheta^k$ $(a_k \in \Delta)$ 的环 $\mathfrak{S}$. 我們来比較 $\mathfrak{S}$ 与一个不定元 x 的多項式环 $\Delta[x]$.

通过映射 $f(x) \to f(\vartheta)$，确切地說：

$$\sum a_k x^k \to \sum a_k\vartheta^k,$$

$\Delta[x]$ 被同态地映到 $\mathfrak{S}$ 上[1]. 于是，根据同态定理，$\mathfrak{S}$ 与一个同余

1) 在非交换情形这一事实不成立，因为尽管变元 x 永远被假定与系数 a_k 可交換，然而量 ϑ 却不一定如此. 仅当 ϑ 与 Δ 的一切元素可交换的特殊情形，这一节的一切討論才成立.

类环同构：

$$\mathfrak{S} \cong \Delta[x]/\mathfrak{p},$$

此处 $\mathfrak{p}$ 是以 ϑ 为零点的那些多項式 $f(x)$（即对于它們来說，$f(\vartheta) = 0$）所成的理想。

因为 $\mathfrak{S}$ 沒有零因子，所以 $\Delta[x]/\mathfrak{p}$ 也不含有零因子，从而理想 $\mathfrak{p}$ 是一个素理想。再者 $\mathfrak{p}$ 不能是单位理想，因为在这个同态之下，单位元 e 不是对应于零而是对应于 e 自身。由于在 $\Delta[x]$ 中每一理想都是主理想，所以只有两个可能：

1. $\mathfrak{p} = (\varphi(x))$，此处 $\varphi(x)$ 是 $\Delta[x]$ 中一个不可分解的多項式[1]。$\varphi(x)$ 是一个具有性質 $\varphi(\vartheta) = 0$ 的最低次多項式。由此推出：

$$\mathfrak{S} \cong \Delta[x]/(\varphi(x)).$$

右端的同余类环是一个域（§ 22）；所以环 $\mathfrak{S}$ 也是一个域。于是 $\mathfrak{S}$ 就是所求的单純扩域 $\Delta(\mathfrak{S})$。

2. $\mathfrak{p} = (0)$。同态 $\Delta[x] \sim \mathfrak{S}$ 变为同构。除零以外，沒有一个多項式 $f(x)$ 具有性質 $f(\vartheta) = 0$，而对于表达式 $f(\vartheta)$，就如同 ϑ 是一个不定元那样来进行运算。在这一情形，环 $\mathfrak{S} \cong \Delta[x]$ 还不是域；然而由这两个环的同构推出它們商域的同构：域 $\Delta(\vartheta)$，环 $\mathfrak{S}$ 的商域与一个不定元 x 的有理函数域同构。

在第一种情形，ϑ 满足 Δ 中的一个代数方程 $\varphi(\vartheta) = 0$，就說 ϑ 对于 Δ 是代数的而域 $\Delta(\vartheta)$ 叫做 Δ 的一个单純代数扩张；在第二种情形，由 $f(\vartheta) = 0$ 得出 $f(x) = 0$，就說 ϑ 对于 Δ 是超越的而域 $\Delta(\vartheta)$ 叫做 Δ 的一个单純超越扩张。根据上述，对于一个超越

---

1) 对于"在 $\Delta[x]$ 中不可分解"，有时也說"在域 Δ 中不可分解"，或者說"在域 Δ 上不可分解"也許更好些。

元素的計算与对于一个不定元的計算一样；我們有 $\Delta(\vartheta)\cong\Delta(x)$.

在代数的情形，根据上述，我們有

$$\Delta(\vartheta)=\mathfrak{S}\cong\Delta[x]/(\varphi(x)),$$

此处 $\varphi(x)$ 是具有零点 ϑ 的最低次（不可分解的）多項式.

在代数的情形，由最后的关系推出下列事实：

a）ϑ 的每一个有理函数也可以写成多項式 $\sum a_k\vartheta^k$.（因为 $\mathfrak{S}$ 被定义作为这样的多項式的全体.）

b）对于这样的多項式的运算同在多項式环 $\Delta[x]$ 中模 $\varphi(x)$ 的同余类的运算一样.

c）方程

$$f(\vartheta)=0$$

可以化为同余式

$$f(x)\equiv 0(\varphi(x)),$$

反过来也对.

d）因为每一多項式模 $\varphi(x)$ 可以化为一个次数 $<n$ 的多項式，这里 n 是 $\varphi(x)$ 的次数，所以 $\Delta(\vartheta)$ 中一切元素可以写成 $\beta=\sum\limits_{k=0}^{n-1}a_k\vartheta^k$ 的形式.

e）因为 ϑ 不滿足低于 n 次的方程，所以 $\Delta(\vartheta)$ 中元素的表示

$$\beta=\sum_{k=0}^{n-1}a_k\vartheta^k$$

是唯一的.

解或根是 ϑ 的不可約方程 $\varphi(x)=0$ 叫做域 $\Delta(\vartheta)$ 的**定义方程**. 多項式 $\varphi(x)$ 的次数叫做代数元素 ϑ 对于 Δ 的**次数**.

当 ϑ 是 Δ 中一个**綫性**方程的解，从而它本身属于 Δ 时，次数是 1. 这时可以取 $\varphi(x)=x-\vartheta$. 因此，上面的命题 c）又重新导出 § 24 中已經証明了的事实：

每一个有零点 ϑ 的多项式可以被 $x-\vartheta$ 整除.

习题. 1. 对于单純代数扩张的情形,直接証明极小多项式 $\varphi(x)$ 的不可約性以及事实 a) 至 e), 即不用同态定理及 $\Delta[x]/(\varphi(x))$ 的域性質来証明. [論斷的次序是:不可約性, c), b), a), d), e). 对于 a) 应用 c).]

2. 进一步証明,除常数因子外, $\varphi(x)$ 是 $\Delta[x]$ 中唯一具有零点 ϑ 的不可約多項式.

3. 下列各域的生成元和它的定义方程是什么:

a) 复数域对于实数域;

b) 域 $\Gamma(\sqrt[3]{3})$ 对于有理数域 Γ;

c) 域 $\Gamma(e^{2\pi i/5})$ 对于有理数域 Γ;

d) 域 $C[i]/(7)$ 对于它所含的素域. ($C[i]$ 是 Gauss 整数环.)

4. 設 Γ 是一个域, z 是一个不定元, $\Sigma=\Gamma(z)$, $\Delta=\Gamma\left(\frac{z^3}{z+1}\right)$. 証明: Σ 是 Δ 的一个单純代数扩张. 元素 z 所滿足的 Δ 中不可約方程是什么?

域 Δ 的两个扩张 Σ, Σ' 説是等价的(对于 Δ), 假如存在一个同构 $\Sigma\cong\Sigma'$, 它把 Δ 的每一元素仍变为自身(保持不动).

域 Δ 的每两个单純超越扩张是等价的.

因为由 $f(x)/g(x)\to f(\vartheta)/g(\vartheta)$, 每一个单純超越扩张 $\Delta(\vartheta)$ 都等价于不定元 x 的有理函数域.

每两个单純代数扩张 $\Delta(\alpha)$, $\Delta(\beta)$ 是等价的,只要 α 与 β 是 $\Delta[x]$ 中同一不可約多項式 $\varphi(x)$ 的零点, 并且此时存在这样的一个同构,它使 Δ 的元素不动而把 α 变到 β.

証明. $\Delta(\alpha)$ 的元素有形状 $\sum_{k=0}^{n-1} a_k\alpha^k$ 而 $\Delta(\beta)$ 的元素有形状 $\sum_{k=0}^{n-1} a_k\beta^k$. 在两个域中, 对于这样的元素的运算和对于多项式模 $\varphi(x)$ 的运算一样. 因此,对应

$$\sum a_k\alpha^k \to \sum a_k\beta^k$$

就是具有所要求性质的一个同构。

一个在 Δ 中不可約的多項式在一个扩域 Ω 中不一定不可約。如果它在 Ω 中有一个零点 ϑ，那末至少分出一个綫性因子 $x-\vartheta$。它在 Ω 中还可能进一步分解成綫性及非綫性因子：

$$\varphi(x)=(x-\vartheta)(x-\vartheta_2)\cdots(x-\vartheta_j)\varphi_1(x)\cdots\varphi_k(x).$$

根据以上的証明，在这一情形，域 $\Delta(\vartheta)$, $\Delta(\vartheta_2)$, $\cdots$, $\Delta(\vartheta_j)$ 都等价，而在同构

$$\Delta(\vartheta)\cong\Delta(\vartheta_2)\cong\cdots\cong\Delta(\vartheta_j)$$

之下，ϑ 变为 ϑ_2, $\cdots$, ϑ_j。

属于一个公共扩域 Ω 的等价的扩张 [象 $\Delta(\vartheta)$, $\Delta(\vartheta_2)$, $\cdots$, $\Delta(\vartheta_j)$ 那样]叫做彼此**共軛**的(对于 Δ)，而在相应的同构之下互相轉变的元素 ϑ, ϑ_2, $\cdots$ 叫做**共軛元素**[1]。由所証明的事实推出：**一个在 $\Delta[x]$ 中不可約多項式 $\varphi(x)$ 在 Ω 中的一切零点对于 Δ 彼此共軛**。反过来，当共軛元素是代数的时侯，永远是同一个不可約多項式 $\varphi(x)$ 的零点；因为由 $\varphi(\vartheta_1)=0$ 推出，当 ϑ_1 通过一个同构变为 ϑ_2 时，正由于这个同构，$\varphi(\vartheta_2)=0$。

单純扩张的存在． 到現在为止，Ω 总被認为是一个預先給定的扩域而单純扩张 $\Delta(\vartheta)$ 是在 Ω 里来研究的。現在将从另一方面提出問題：域 Δ 是給定的；而一个扩域 $\Delta(\vartheta)$ 是所求的，此外又要求或者 ϑ 是超越的，或者 ϑ 是一个預先給定在 $\Delta[x]$ 中不可約多項式的零点。

如果 ϑ 是超越的，那末間題的解是容易的：对于 ϑ，我們取一个不定元

$$\vartheta=x,$$

1) 这种記法主要是对代数元素 ϑ 应用的。同一域的超越元素永远彼此等价。

作多項式环 $\Delta[x]$ 和它的商域 $\Delta(x)$，不定元 x 的有理函数域. 如我們所知，除等价扩张外，$\Delta(x)$ 是唯一的单純超越扩张；于是有：

一个給定域 Δ 的单純超越扩张存在一个，而且除等价扩张外，只存在一个.

其次設 ϑ 是代数的，并且是 $\Delta[x]$ 中不可約多項式 $\varphi(x)$ 的一个零点，那末我們可以首先假設 φ 不是綫性的，否則就可以取 $\Delta(\vartheta)=\Delta$.

根据上述，所求的域必定与同余类环

$$\Sigma' = \Delta[x]/(\varphi(x))$$

同构. 现在对于 $\Delta[x]$ 中每一多項式 f，有 Σ' 中一个同余类 $\bar{f}$ 与它对应，并且这个映射是一个同态映射. 特别，对于 Δ 的每一常数 a 有一个同余类 $\bar{a}$ 与它对应，而 Δ 的这个映射不但是同态，而且是同构，因为零是唯一的常数 $\equiv 0 \bmod \varphi(x)$. 于是根据 § 15 末尾，在域 Σ' 中同余类 $\bar{a}$ 可以用它所对应的 Δ 的元素 a 来代换；从而 Σ' 变为一个包含 Δ 且 $\cong \Sigma'$ 的域 Σ.

有一个同余类与多項式 x 对应，我們可以称它为 ϑ. 于是可以在 Σ 中作出域 $\Delta(\vartheta)$. [容易看出，$\Sigma=\Delta(\vartheta)$.] 由

$$\varphi(x)=\sum_0^n a_k x^k \equiv 0(\varphi(x)),$$

借助于同态，我們得出

$$\sum_0^n \bar{a}_k \vartheta^k = 0 \quad (\text{在 } \Sigma' \text{ 内}),$$

于是，当 $\bar{a}_k$ 被 a_k 代換时，将有

$$\varphi(\vartheta)=\sum_0^n a_k\vartheta^k=0.$$

所以 ϑ 是 $\varphi(x)$ 的零点.

这样就証明了：

对于一个給定的域Δ存在一个(并且除等价扩张外，只存在一个)单純代数扩张$\Delta(\vartheta)$，使得ϑ满足一个給定的在$\Delta[x]$中不可約方程$\varphi(x)=0$.

在証明中借助于同余类环与符号ϑ所用的“符号添加”过程在某种程度上是关于非符号添加的逆命题，后者当我們开始就有一个包括域Ω，在其中已經存在一个具有所要求性质的元素ϑ的时候是可能的。例如，若Δ是有理数域，那末一个代数数(即一个代数方程的根)的非符号添加可以从利用超越方法所作的复数域出发而达到，在复数域中，根据“代数基本定理”，每一个具有理数系数的方程实际上是可解的。上面的符号添加避免了这种超越的迂迴途径，而是直接把代数数当作一个同余类的符号来引入，并且对它定义运算規則。在这里并沒有引入大小关系($>$，$<$)或实数性质。虽然如此，由符号的或非符号超越途径都作成(就代数来說)同一个域$\Delta(\vartheta)$；因为根据开始所証，当ϑ满足同一个不可約方程时，一切可能的扩张$\Delta(\vartheta)$是等价的。这样，符号添加与非符号添加都容納在§34的一般的添加概念之下；唯一的差別就是对于添加所要求的包括域Ω或Σ，在一种情形是已知的，而另一种情形是需要首先作出的。

关于量的大小与代数关系之間的联系的詳細情形将在第九章与第十章中找到。

习題. 5. 多項式x^4+1在有理数域Γ中不可約(§27，习題3)。添加一个零点ϑ并且把这个多項式在扩域$\Gamma(\vartheta)$中分解成素因子。

6. 令Π是特征p的素域，x是一个不定元，$\Delta=\Pi(x)$。对于Δ添加不可約多項式z^p-x的一个零点$\zeta=x^{1/p}$并且在扩域$\Pi(\zeta)$中分解多項式z^p-x。

7. 由特征2的素域，通过添加一个不可約二次方程的一个零点，作一个

含有四个元素的域。

§ 36. 体上的綫性相关性

設 $\mathfrak{G}$ 是一个模，即一个 Abel 加羣，元素为 $u, v, \cdots$，又設 Δ 是一个体，元素为 $\alpha, \beta, \cdots$.

設(如同 § 17 那样)有一个乘法 αv 被定义，具有下列性質：

1. αv 永远属于 $\mathfrak{G}$,
2. $\alpha(u+v)=\alpha u+\alpha v$,
3. $(\alpha+\beta)u=\alpha u+\beta u$,
4. $(\alpha\beta)u=\alpha(\beta u)$,
5. $1u=u$.

在应用上，首先使我們感兴趣的是 $\mathfrak{G}$ 是 Δ 的一个扩体. 然而我們有意地将假設提得如此广泛，使得其他加羣，例如，Δ 上的向量空間，Δ 上的代数以及任意一个包含 Δ 的环都可以列入.

$\mathfrak{G}$ 的一个元素 v 說是与元素 $u_1, \cdots, u_n$ 綫性相关(对于 Δ)，假如

$$v=\alpha_1u_1+\cdots+\alpha_nu_n,$$

或者，用同样的話来說，如果存在一个綫性关系

$$\beta_0v+\beta_1u_1+\cdots+\beta_nu_n=0,$$

而 $\beta_0\neq 0$. 特别，当 $v=0$ 时，就說 v 与空集綫性相关.

对于綫性相关的概念有一系列的定理成立，以下将分为"基础定理"与"导出定理"来提出. 基础定理直接由概念的定义导出. 相反地，导出定理則是由基础定理导出，而不必再应用定义，因而不必再考虑"綫性相关性"概念的意义. 这种方法(我們可以称它为綫性相关性概念的公理化)在考虑到以后一章时(第八章，§ 64)是有用的，在那里将引入"代数相关性"的概念，对于这一概念来

說，和綫性相关性概念同样的基础定理成立，因而同样的导出定理也成立。

三个基础定理就足够了。第一个是自明的。

基础定理 1. 每一 $u_i(i=1,\cdots,n)$ 与 $u_1,\cdots,u_n$ 綫性相关。

基础定理 2. 若 v 与 $u_1,\cdots,u_n$ 綫性相关，而不与 $u_1,\cdots,u_{n-1}$ 綫性相关，那末 u_n 与 $u_1,\cdots,u_{n-1},v$ 綫性相关。

証明． 在方程

$$\beta_0 v+\beta_1 u_1+\cdots+\beta_n u_n=0 \quad (\beta_0\neq 0)$$

中，必須 $\beta_n\neq 0$，否則 v 将与 $u_1,\cdots,u_{n-1}$ 綫性相关。

基础定理 3. 若 w 与 $v_1,\cdots,v_s$ 綫性相关及每一 $v_j(j=1,\cdots,s)$ 与 $u_1,\cdots,u_n$ 綫性相关，那末 w 与 $u_1,\cdots,u_n$ 綫性相关。

証明． 由 $w=\sum_i \alpha_i v_i$ 及 $v_i=\sum_k \beta_{ik}u_k$ 推出

$$w=\sum_i \alpha_i\Big(\sum_k \beta_{ik}u_k\Big)=\sum_{i,k}\alpha_i\beta_{ik}u_k=\sum_k\Big(\sum_i \alpha_i\beta_{ik}\Big)u_k.$$

由基础定理 1 及 3 推出

导出定理 1. 若 w 与 $v_1,\cdots,v_s$ 綫性相关，那末 w 也与任何一个包有 $\{v_1,\cdots,v_s\}$ 的組 $\{u_1,\cdots,u_n\}$ 綫性相关。

当 $v_1,\cdots,v_s$ 除次序外与 $u_1,\cdots,u_n$ 一致时，就給出一个特殊情形。因此，綫性相关的概念不依賴于 $u_1,\cdots,u_n$ 的次序。

定义. 元素 $u_1,\cdots,u_n$ 說是綫性无关，假如其中沒有一个元素与其余元素綫性相关。

这就意味着（然而在推导导出定理时，并沒有使用这个意义）在每一关系

$$\alpha_1 u_1+\cdots+\alpha_n u_n=0$$

中必須 $\alpha_1=0,\cdots,\alpha_n=0$。綫性无关的概念不依賴于 $u_1,\cdots,u_n$

的次序．空集永远叫作綫性无关的．单独一个元素 u，当它与空集无关，因而 $u \neq 0$ 时，是綫性无关的．

导出定理 2. 若 $u_1, \cdots, u_{n-1}$ 綫性无关而 $u_1, \cdots, u_{n-1}, u_n$ 则不然，那末 u_n 与 $u_1, \cdots, u_{n-1}$ 綫性相关．

証明． 在元素 $u_1, \cdots, u_{n-1}, u_n$ 之中必有一个与其余的綫性相关．如果这个元素是 u_n，那末我們已經証完了．若不是 u_n 而是，例如，u_{n-1}，那末 u_{n-1} 与 $u_1, \cdots, u_{n-2}, u_n$ 綫性相关而不与 $u_1, \cdots, u_{n-2}$ 綫性相关，从而（基础定理 2）u_n 与 $u_1, \cdots, u_{n-1}$ 綫性相关．

导出定理 3. 有限多个元素 $u_1, \cdots, u_n$ 的組含有一个（可能是空的）綫性无关部分組，而一切 $u_i (i = 1, \cdots, n)$ 都与它綫性相关．

証明． 由这一組中选出一个含有尽可能多的綫性无关元素的部分組．每一个含于这个部分組內的 u_i，根据基础定理 1，而每一不含于这个部分組內的 u_j，根据导出定理 2，与这一部分組綫性相关．

定义. 两个有限組 $u_1, \cdots, u_r$ 与 $v_1, \cdots, v_s$ 說是（綫性）等价的，假如每一 v_k 与 $u_1, \cdots, u_r$ 綫性相关，而每一 u_i 与 $v_1, \cdots, v_s$ 綫性相关．

根据定义，等价关系是对称的，根据基础定理 1，是自反的，而根据基础定理 3，是传递的．如果一个元素 w 与两个等价組之中的一个綫性相关，那末根据基础定理 3，它也与另一个綫性相关．根据导出定理 3，每一有限組等价于一个綫性无关部分組．

导出定理 4（替换定理）. 設 $v_1, \cdots, v_s$ 綫性无关而每一 v_j 与 $u_1, \cdots, u_r$ 綫性相关，那末在 u_i 的組里，存在一个恰好含有 s 个元素的部分組 $\{u_{i_1}, \cdots, u_{i_s}\}$，可以把它用 $\{v_1, \cdots, v_s\}$ 来替换，使得由 $\{u_1, \cdots, u_r\}$ 通过替换所得的組与原来的組 $\{u_1, \cdots, u_r\}$

等价．由此特别有 $s \leqslant r$.

証明． 对于 $s=0$，論断是明显的：这时沒有 v_j 而且沒有什么可替换的． 假設論断对于 $\{v_1, \cdots, v_{s-1}\}$ 已經被証明，并且假設 $\{v_1, \cdots, v_{s-1}\}$ 被 $\{u_{i_1}, \cdots, u_{i_{s-1}}\}$ 替换． 通过这一替换，形成一个与 $\{u_1, \cdots, u_r\}$ 等价的組 $\{v_1, \cdots, v_{s-1}, u_k, u_l, \cdots\}$． 現在 v_s 与 $\{u_1, \cdots, u_r\}$ 綫性相关，从而也与等价組 $\{v_1, \cdots, v_{s-1}, u_k, u_l, \cdots\}$ 綫性相关． 因此又存在 $\{v_1, \cdots, v_{s-1}, u_k, u_l, \cdots\}$ 的一个极小部分組，而 v_s 仍与它綫性相关． 这个极小部分組不能完全由 v_j 組成，因为 v_j 与 v_s 綫性无关． 因此极小部分組 $\{v_j, \cdots, u_k\}$ 至少含有一个 u_k，我們叫他做 u_{i_s}． 根据基础定理 2，$u_k = u_{i_s}$ 与由 $\{v_j, \cdots, u_k\}$ 通过以 v_s 替换 u_k 所形成的組綫性相关，因而也与它的包括組綫性相关，这个包括組是由 $\{v_1, \cdots, v_{s-1}, u_k, u_l, \cdots\}$ 通过替换 $u_k \to v_s$ 而形成的． 令这一組是 $\{v_1, \cdots, v_{s-1}, v_s, u_l, \cdots\}$． 它与 $\{v_1, \cdots, v_{s-1}, u_k, u_l, \cdots\}$ 等价，因为 u_k 与前一組綫性相关，而 v_s 也与后一組綫性相关． 这样，我們又将替换向前推进一步． 新的組 $\{v_1, \cdots, v_{s-1}, v_s, u_l, \cdots\}$ 与 $\{v_1, \cdots, v_{s-1}, u_k, u_l, \cdots\}$ 等价，从而也与原来的組 $\{u_1, \cdots, u_r\}$ 等价．

导出定理 5. 两个等价的綫性无关組 $\{u_1, \cdots, u_r\}$ 与 $\{v_1, \cdots, v_s\}$ 由相同个数的元素組成．

証明． 根据导出定理 4 有 $s \leqslant r$ 及 $r \leqslant s$.

定义． $\mathfrak{S}$ 中一个集 $\mathfrak{M}$ 叫做对于体 Δ 来說是有限秩的，或者簡称在 Δ 上有限的，假如这个集的一切元素都与其中有限个元素綫性相关． 例如，单純代数扩张 $\Delta(\vartheta)$ 在 Δ 上有限，因为根据 § 35，$\Delta(\vartheta)$ 的一切元素都可以由 $1, \vartheta, \vartheta^2, \cdots, \vartheta^{n-1}$ 綫性表示． 一般来說，Δ 上每一个代数是有限秩的．

根据导出定理 3，我們可以从使得 $\mathfrak{M}$ 中一切元素与它們綫性相

关的有限个元素中选出一个等价的綫性无关部分組 $\{u_1, \cdots, u_r\}$. 这样的一个綫性无关部分組，对于它来說，$\mathfrak{M}$ 中一切元素与它綫性相关，叫做 $\mathfrak{M}$ 的一个**基**，确切地說，一个 Δ-**基**（也叫做 $\mathfrak{M}$ 的一个"极小基"或"綫性无关基"）.

如果把 $\mathfrak{M}$ 的元素通过基元素表出：

$$u = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_r u_r, \tag{1}$$

那末系数 $\alpha_1, \cdots, \alpha_r$ 是唯一确定的；因为由

$$\alpha_1 u_1 + \cdots + \alpha_r u_r = \beta_1 u_1 + \cdots + \beta_r u_r$$

推出

$$\sum_i (\alpha_i - \beta_i) u_i = 0,$$

从而由綫性无关性

$$\alpha_i - \beta_i = 0.$$

反过来，由表示 (1) 的唯一性推出基元素的綫性无关性.

根据导出定理 5，$\mathfrak{M}$ 中每一基的基元素的个数是相同的. 这个个数叫做 $\mathfrak{M}$ 对于 Δ 的**綫性秩**并且記作 $(\mathfrak{M}:\Delta)$. 在 Δ 上的有限扩体 $\mathfrak{M}$ 的情形，綫性秩 $(\mathfrak{M}:\Delta)$ 也叫做 $\mathfrak{M}$ 在 Δ 上的**体次数**. 在向量空間 $\mathfrak{M}$ 的一般情形，$(\mathfrak{M}:\Delta)$ 也叫做 $\mathfrak{M}$ 的**維数**.

若 r 是 $\mathfrak{M}$ 的綫性秩，那末根据导出定理 4，对于 $\mathfrak{M}$ 中每一綫性无关組 $v_1, \cdots, v_s$ 来說，不等式 $s \leqslant r$ 成立. 因此綫性秩也可以定义作为这个集中綫性无关元素的最大个数. 由此推出

导出定理 6. 对于 Δ 是有限的集 $\mathfrak{M}$ 的一个子集 $\mathfrak{N}$ 仍是有限的，并且 $\mathfrak{N}$ 的綫性秩最高等于 $\mathfrak{M}$ 的綫性秩.

习题. 1. 若 r 是 $\mathfrak{M}$ 的秩，那末任意 r 个綫性无关的元素都作成一个基.

2. 当 $\mathfrak{M}$ 有有限秩时，$\mathfrak{M}$ 的一个子集 $\mathfrak{N}$ 的每一个基可以扩充为 $\mathfrak{M}$ 的一个基.

3. 由 $\mathfrak{S} \supseteq \Delta$ 及 $(\mathfrak{S}:\Delta)=1$ 推出 $\mathfrak{S}=\Delta$.

现在我們特别将綫性秩的概念应用到体 Δ 的这样一个扩体上,它在 Δ 上是有限的. 对于域来說,綫性秩 $(\Sigma:\Delta)$ 一般地叫做 Σ 在 Δ 上的次数. 当次数有值 2, 3, 4 时,就説是二次, 三次, 四次扩域. 由一个 n 次代数元生成的单純代数扩张 $\Sigma=\Delta(\vartheta)$ 是有限的并且有次数 n, 因为綫性无关幂 $1, \vartheta, \vartheta^2, \cdots, \vartheta^{n-1}$ 作成一个基.

設 Σ 是 Δ 与 Ω 間的一个中間域,即 $\Delta \subseteq \Sigma \subseteq \Omega$. 那末以下定理成立:

定理. 若 Ω 在 Δ 上有限, 那末 Σ 也在 Δ 上有限且 Ω 也在 Σ 上有限. 反过来,若 Σ 在 Δ 上有限且 Ω 在 Σ 上有限,那末 Ω 在 Δ 上有限并且次数关系

$$(\Omega:\Delta)=(\Omega:\Sigma)(\Sigma:\Delta) \tag{2}$$

成立.

証明. 若 Ω 在 Δ 上有限,那末根据导出定理 6, Σ 也在 Δ 上有限. Ω 在 Σ 上有限是明显的,因为 Ω 已經在 Δ 上有限. 现在反过来設 $(\Sigma:\Delta)$ 与 $(\Omega:\Sigma)$ 都是有限的并且設 $\{u_1, \cdots, u_r\}$ 是 Σ 对于 Δ 的一个基而 $\{v_1, \cdots, v_s\}$ 是 Ω 对 Σ 的一个基. 那末 Ω 的每一元素可以被表示成以下形式:

$$\begin{aligned} w &= \sum_i \sigma_i v_i & (\sigma_i \in \Sigma) \\ &= \sum_i \Big(\sum_k \delta_{ik} u_k\Big) v_i & (\delta_{ik} \in \Delta) \\ &= \sum_i \sum_k \delta_{ik}(u_k v_i). \end{aligned}$$

因此 Ω 的每一元素与 rs 个元素 $u_k v_i$ 綫性相关. 这些元素对于 Δ 彼此綫性无关;因为由

$$\sum_i \sum_k \delta_{ik} u_k v_i = 0, \qquad (\delta_{ik} \in \Delta)$$

根据 v 对于 Σ 的綫性无关性，推出

$$\sum_k \delta_{ik} u_k = 0,$$

于是根据 u 对于 Δ 的綫性无关性，

$$\delta_{ik} = 0.$$

所以 rs 是 Ω 对于 Δ 的次数，証毕.

由 (2) 的推論：

a) 若 $\Delta \subseteq \Sigma \subseteq \Omega$ 而 $(\Omega:\Delta) = (\Sigma:\Delta)$，那末 $\Omega = \Sigma$. 因为这时由 (2) 就推出 $(\Omega:\Sigma) = 1$. 同样：

b) 若 $\Delta \subseteq \Sigma \subseteq \Omega$ 而 $(\Omega:\Sigma) = (\Omega:\Delta)$，那末 $\Sigma = \Delta$.

c) 若 $\Delta \subseteq \Sigma \subseteq \Omega$，那末次数 $(\Sigma:\Delta)$ 是次数 $(\Omega:\Delta)$ 的一个因子.

习題. 4. 域 $\Gamma(i, \sqrt{2})$ 对于有理数域 Γ 的次数是什么?

5. 域 Δ 的有限扩域 Ω 中一切元素对于 Δ 来說都是代数的，并且它們的次数是域次数 $(\Omega:\Delta)$ 的一个因子.

6. 如果一个特征 p 的域对于它所包含的素域的次数是 n，那末它是由多少元素組成的?

§ 37. 体上的綫性方程組

綫性相关性理論的一个重要应用就是綫性方程組的解理論.

設 $l_1, \cdots, l_m$ 是系数在一个体 Δ 內关于不定元 $x_1, \cdots, x_n$ 的綫性齐式：

(1) $$l_i = \Sigma \alpha_{ik} x_k.$$

又設 $\beta_1, \cdots, \beta_m$ 是 Δ 中給定的元素. 我們来寻求(在 Δ 內)方程組

(2) $$l_i(\zeta) = \Sigma \alpha_{ik} \zeta_k = \beta_i \quad (i = 1, 2, \cdots, m).$$

的所有解 $(\zeta_1, \cdots, \zeta_n)$.

在綫性齐式 $l_1, \cdots, l_m$ 中綫性无关的个数 r 叫做这个方程組的秩. 我們設想如此选择綫性齐式 l_i 的号碼，使得 $l_1, \cdots, l_r$ 綫性无关而其余 l_i 由它們綫性表示：

$$(3) \qquad l_i = \sum_1^r s_{ik} l_k \quad (i = r + 1, \cdots, m).$$

当把在 l_i 中所出現的 x_j 用 ζ_j 来代替时，关系式(3)仍然保持正确. 現在方程組(2)可解的必要条件是，把 l_i 換成 β_i，这个关系式也保持正确：

$$(4) \qquad \beta_i = \sum_1^r s_{ik} \beta_k \quad (i = r + 1, \cdots, m).$$

如果这些条件都被滿足，那末(2)的一切方程都是其中前 r 个方程的結果. 因此我們只需研究这 r 个綫性无关的方程.

綫性齐式 $l_1, \cdots, l_r$ 与不定元 $x_1, \cdots, x_n$ 綫性相关. 于是根据替換定理(§ 36, 导出定理 4)，我們可以把不定元中的 r 个，例如（适当地編号）$x_1, \cdots, x_r$ 用 $l_1, \cdots, l_r$ 替換，使得这个新組 $\{l_1, \cdots, l_r, x_{r+1}, \cdots, x_n\}$ 与組 $\{x_1, \cdots, x_n\}$ 等价. 这就是說，所有的 x 都与 $l_1, \cdots, l_r, x_{r+1}, \cdots, x_n$ 綫性相关：

$$(5) \qquad x_i = \sum_1^r \gamma_{ij} l_j + \sum_{r+1}^n \delta_{ik} x_k \quad (i = 1, \cdots, r).$$

这个关系当以 ζ_i 代替 x_i 并且以 β_j 代替 l_j 时也必須成立：

$$(6) \qquad \zeta_i = \sum_1^r \gamma_{ij} \beta_j + \sum_{r+1}^n \delta_{ik} \zeta_k \quad (i = 1, \cdots, r).$$

因此这 r 个未知量 $\zeta_1, \cdots, \zeta_r$ 可以由其余的未知量 $\zeta_{r+1}, \cdots, \zeta_n$ 綫性表示.

到此为止我們只建立了所給的綫性方程組的一切解所必須滿

足的必要条件. 我們断言,这个必要条件也是充分的:

当条件(4)被满足时,方程組(2)可解,这个解可以由公式(6)求出,其中 $\zeta_{r+1}, \cdots, \zeta_n$ 可以任意选取.

証明. 因为組 $\{l_1, \cdots, l_r, x_{r+1}, \cdots, x_n\}$ 与組 $\{x_1, \cdots, x_n\}$ 等价,所以它有同一秩 n,又因为这一組恰好含有 n 个元素,所以这些元素綫性无关. 因此,若把(3)及(5)代入(1),就得到一个 $l_1, \cdots, l_r, x_{r+1}, \cdots, x_n$ 的恆等式,这个恆等式当以 $\beta_1, \cdots, \beta_r$ 代替 $l_1, \cdots, l_r$ 并且以任意元素 $\zeta_{r+1}, \cdots, \zeta_n$ 代替 $x_{r+1}, \cdots, x_n$ 时仍然成立. 这就是說,由(4)所确定的 β_i 与由(6)所确定的 ζ_i 的确满足方程(2).

为了实际确定秩 r,为了寻求綫性无关的 l_i 以及为了建立解的公式(6),我們利用(在实际上也是如此)逐次消去法:首先将关系式(1)中之一对一个 x_j 解出,把这个 x_j 代入(1)的其他关系式中,从而有一个基元素 x_j 被 l_i 所代替,如此継續下去,直到在对于还可能存留的 l_i 的表示式中不再出现 x 时为止,从而这些 l_i 只依赖于(我們說) $l_1, \cdots, l_r$. 于是我們能够确定,所求的綫性关系(3)是否对于 β_i 也成立,或者,一开始在計算时就用已知的 β_i 来代替 l_i 更为方便. 公式(5)或(以 β 代替 l 并且以 ζ 代替 x 之后)解的公式(6)通过逐次代入完全自动地得出.

由这个有理运算的可能性得出:当一个綫性方程組的系数属于 Δ 的一个子体时,那末解的公式(6)的系数也在同一体內. 如果这个方程組在 Δ 中可解,那末它已經在子体內已經可解.

在齐次方程組的特殊情形(一切 $\beta_i = 0$),必要条件(4)自动地满足. 因此齐次方程組永远可解并且解由公式(6)給出,其中 $\beta_i = 0$. 在这一情形,(6)也可以这样解释:所有解向量都是 $n - r$ 个特殊解向量

$$(\delta_{1r+1}, \delta_{2r+1}, \cdots, \delta_{rr+1}, 1, 0, \cdots, 0)$$
$$(\delta_{1r+2}, \delta_{2r+2}, \cdots, \delta_{rr+2}, 0, 1, \cdots, 0)$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$(\delta_{1n}, \delta_{2n}, \cdots, \delta_{rn}, 0, 0, \cdots, 1)$$

的綫性組合并且这些解可以由依次以完全任意的元素 $\zeta_{r+1}, \cdots, \zeta_n$ 从右边去乘这些向量再相加得出. 在 $r=n$ 的特殊情形只有"平凡解"$(0, \cdots, 0)$.

在域的情形，行列式理論提供了明显的解的公式以及綫性方程的可解性与綫性相关性的代数判定标准，对此可参考有关的教科书.

§38. 域的代数扩张

Δ 的一个扩域 Σ 叫做在 Δ 上是代数的，假如 Σ 的每一元素都是 Δ 上的代数元素.

定理. Δ 的每一有限扩域都是代数的，并且可以由 Δ 通过添加有限个代数元素而得到.

証明. 設 n 是有限扩域 Σ 的次数又 $\alpha \in \Sigma$，那末在元素 α 的幂 $1, \alpha, \alpha^2, \cdots, \alpha^n$ 中至多有 n 个是綫性无关的. 因此必定有一个关系 $\sum_{0}^{n} c_k\alpha^k$ 成立，即 α 是代数的；从而域 Σ 是代数的. 作为域 Σ 的生成元(即作为添加的集)，我們可以选取 Σ 的一个域基.

由于这个定理，代替"有限扩张"，我們也可以說"有限代数扩张".

逆定理. 域 Δ 的每一个通过对 Δ 添加有限个代数元而生成的扩张是有限的(从而是代数的).

証明. 添加一个 n 次代数元 ϑ 生成一个具有基 $1, \vartheta, \cdots, \vartheta^{n-1}$ 的有限扩张. 根据 §36 的最后定理，依次构成有限扩张仍旧

生成一个有限扩张.

推論. 代数元素的和,差,积,商仍是代数元素.

定理. 若 α 对于 Σ 是代数的,而 Σ 对于 Δ 是代数的,那末 α 对于 Δ 是代数的.

証明. 在对于 α 的系数取自 Σ 的代数方程里只可能有 Σ 的有限个元素 $\beta, \gamma, \cdots$ 作为系数出現. 域 $\Sigma' = \Delta(\beta, \gamma, \cdots)$ 对于 Δ 是有限的而域 $\Sigma'(\alpha)$ 对于 Σ' 是有限的;因此 $\Sigma'(\alpha)$ 对于 Δ 也是有限的,从而 α 对于 Δ 是代数的.

分裂域. 在有限代数扩张中,一个多項式 $f(x)$ 的"分裂域"特别重要,它是通过"添加方程 $f(x) = 0$ 的一切根"而生成的. 因此分裂域是这样一个域 $\Delta(\alpha_1, \cdots, \alpha_n)$, 在其中 $\Delta[x]$ 的多項式 $f(x)$ 完全分解成綫性因子[1]:

$$f(x) = (x - \alpha_1)\cdots(x - \alpha_n),$$

并且通过对 Δ 添加这些綫性因子的根 α_i 而生成的. 关于这个域以下定理成立:

对于 $\Delta[x]$ 中每一多項式 $f(x)$ 都存在一个分裂域.

証明. 在 $\Delta[x]$ 中 $f(x)$ 可以分解成不可約因子如下:

$$f(x) = \varphi_1(x)\varphi_2(x)\cdots\varphi_r(x).$$

現在首先添加不可約多項式 $\varphi_1(x)$ 的一个零点 α_1, 由此得到一个域 $\Delta(\alpha_1)$, 在其中 $\varphi_1(x)$,从而 $f(x)$ 分裂出一个綫性因子 $x - \alpha_1$.

假設已經作出一个域 $\Delta_k = \Delta(\alpha_1, \cdots, \alpha_k)\,(k < n)$, 在其中多項式 $f(x)$ 分裂出(相同或不同的)因子 $x - \alpha_1, \cdots, x - \alpha_k$. 在域 Δ_k 中 $f(x)$ 可以如下地分解:

$$f(x) = (x - \alpha_1)\cdots(x - \alpha_k)\cdot\psi_{k+1}(x)\cdots\psi_l(x).$$

---

[1] 在这里和以后都将假定 $f(x)$ 的最高系数是 1,这显然是无关紧要的.

現在对 Δ_k 添加 $\phi_{k+1}(x)$ 的一个零点 α_{k+1}. 在这样扩张的域 $\Delta_k(\alpha_{k+1})=\Delta(\alpha_1, \cdots, \alpha_{k+1})$ 中，$f(x)$ 分裂出因子 $x-\alpha_1, \cdots, x-\alpha_{k+1}$. 由这个添加，$f(x)$ 也許可能还分裂出多于 $k+1$ 个因子.

按这种方法逐步繼續下去，最后得出所求的域 $\Delta_n=\Delta(\alpha_1, \cdots, \alpha_n)$[1].

我們現在将进一步指出，一个給定的多項式 $f(x)$ 的分裂域除等价扩张外是唯一确定的. 为此需要应用同构的开拓这一概念.

設 $\Delta\subseteq\Sigma$ 及 $\bar{\Delta}\subseteq\bar{\Sigma}$，又設給定了一个同构 $\Delta\cong\bar{\Delta}$. 一个同构 $\Sigma\cong\bar{\Sigma}$ 叫做所給的同构 $\Delta\cong\bar{\Delta}$ 的开拓，假如 Δ 中每一元素 a，在旧同构 $\Delta\cong\bar{\Delta}$ 之下有象 $\bar{a}$，在新同构 $\Sigma\cong\bar{\Sigma}$ 之下也有 $\bar{\Delta}$ 中同一象 $\bar{a}$.

在代数扩张中有关同构开拓的一切定理都建立在以下定理的基础上：

若在一个同构 $\Delta\cong\bar{\Delta}$ 之下 $\Delta[x]$ 中一个不可約多項式 $\varphi(x)$ 映成 $\bar{\Delta}[x]$ 中多項式 $\bar{\varphi}(x)$（自然同样也是不可約的），又設 α 是 $\varphi(x)$ 在 Δ 的一个扩域中的一个零点而 $\bar{\alpha}$ 是 $\bar{\varphi}(x)$ 在 $\bar{\Delta}$ 的一个扩域中的一个零点，那末所給的同构 $\Delta\cong\bar{\Delta}$ 可以开拓成一个同构 $\Delta(\alpha)\cong\bar{\Delta}(\bar{\alpha})$，它把 α 映成 $\bar{\alpha}$.

証明. $\Delta(\alpha)$ 的元素有形式 $\Sigma c_k\alpha^k (c_k\in\Delta)$，而对它們的运算与对多項式模 $\varphi(x)$ 的运算一样. 同样，$\bar{\Delta}(\bar{\alpha})$ 的元素有形式 $\Sigma\bar{c}_k\bar{\alpha}^k (\bar{c}_k\in\bar{\Delta})$，而对它們的运算与对多項式模 $\bar{\varphi}(x)$ 的运算一样，因此，除了一个横綫外，是完全同样的. 所以对应

$$\Sigma c_k\alpha^k\rightarrow\Sigma\bar{c}_k\bar{\alpha}^k$$

1）这里所給出的分裂域的存在証明并不蘊涵在有限步下实际构成的可能性. 关于这个問題請看 G. Hermann, *Math. Ann.*, **95** (1926), 736—788 及 B. L. v. d. Waerden, *Math. Ann.*, **102** (1930), 738.

(此处 $\bar{c}_k$ 是在同构 $\Delta\cong\bar{\Delta}$ 之下与 c_k 对应的元素)是一个具有所要求性質的同构.

特別，若 $\Delta=\bar{\Delta}$ 且所給的同构把 Δ 的每一个元素映到自身，那末再一次得到以前的定理，卽添加同一不可約方程的根所生成的一切扩张 $\Delta(\alpha)$, $\Delta(\bar{\alpha})$, $\cdots$ 是等价的，并且每一根由相应的同构变为其他的每一根.

相应的定理对于添加一个多項式的全部根以代替添加一个根也成立:

若在一个同构 $\Delta\cong\bar{\Delta}$ 之下，$\Delta[x]$ 中任意多項式 $f(x)$ 映成 $\bar{\Delta}[x]$ 中一个多項式 $\bar{f}(x)$，那末这个同构可以开拓成 $f(x)$ 的任意分裂域 $\Delta(\alpha_1,\cdots,\alpha_n)$ 与 $\bar{f}(x)$ 的任意分裂域 $\bar{\Delta}(\bar{\alpha}_1,\cdots,\bar{\alpha}_n)$ 的一个同构，其中 $\alpha_1,\cdots,\alpha_n$ 按某种次序映成 $\bar{\alpha}_1,\cdots,\bar{\alpha}_n$.

証明. 假設已經(可能改变一下根的次序)把同构 $\Delta\cong\bar{\Delta}$ 开拓成一个同构 $\Delta(\alpha_1,\cdots,\alpha_k)\cong\bar{\Delta}(\bar{\alpha}_1,\cdots,\bar{\alpha}_k)$，其中每一 α_i 映成 $\bar{\alpha}_i$.(对于 $k=0$ 来說实际就是这样.)在 $\Delta(\alpha_1,\cdots,\alpha_k)$ 中 $f(x)$ 可以如此分解:

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_k)\cdot\varphi_{k+1}(x)\cdots\varphi_h(x).$$

于是，借助于同构，$\bar{f}(x)$ 在域 $\bar{\Delta}(\bar{\alpha}_1,\cdots,\bar{\alpha}_k)$ 中相应地分解如下:

$$\bar{f}(x)=(x-\bar{\alpha}_1)\cdots(x-\bar{\alpha}_k)\cdot\bar{\varphi}_{k+1}(x)\cdots\bar{\varphi}_h(x).$$

在 $\Delta(\alpha_1,\cdots,\alpha_n)$ 及 $\bar{\Delta}(\bar{\alpha}_1,\cdots,\bar{\alpha}_n)$ 中，因子 φ_ν 与 $\bar{\varphi}_\nu$ 又分别分解为 $(x-\alpha_{k+1})\cdots(x-\alpha_n)$ 及 $(x-\bar{\alpha}_{k+1})\cdots(x-\bar{\alpha}_n)$. α_{k+1}, $\cdots$, α_n 与 $\bar{\alpha}_{k+1}$, $\cdots$, $\bar{\alpha}_n$ 可以这样排列，使得 α_{k+1} 是 $\varphi_{k+1}(x)$ 的根而 $\bar{\alpha}_{k+1}$ 是 $\bar{\varphi}_{k+1}(x)$ 的根. 根据上面的定理，同构

$$\Delta(\alpha_1,\cdots,\alpha_k)\cong\bar{\Delta}(\bar{\alpha}_1,\cdots,\bar{\alpha}_k)$$

可以开拓成

$$\Delta(\alpha_1,\cdots,\alpha_{k+1})\cong\bar{\Delta}(\bar{\alpha}_1,\cdots,\bar{\alpha}_{k+1}),$$

其中 α_{k+1} 映成 $\bar{\alpha}_{k+1}$.

从 $k=0$ 开始,按这样的方法一步一步地継續下去,最后得到所求的同构

$$\Delta(\alpha_1, \cdots, \alpha_n) \cong \bar{\Delta}(\bar{\alpha}_1, \cdots, \bar{\alpha}_n),$$

根据这种构成,每一 α_i 映成 $\bar{\alpha}_i$.

現在,特别若 $\Delta = \bar{\Delta}$ 并且所給的同构 $\Delta \cong \bar{\Delta}$ 使 Δ 中每一元素不变,那末 $f = \bar{f}$ 并且扩充了的同构

$$\Delta(\alpha_1, \cdots, \alpha_n) \cong \Delta(\bar{\alpha}_1, \cdots, \bar{\alpha}_n)$$

同样也使 Δ 的一切元素不变,这就是說,$f(x)$ 的两个分裂域是等价的. 因此,一个多項式 $f(x)$ 的分裂域除等价扩张外是唯一确定的.

由此推出,根的一切代数性質不依賴于分裂域的构成方法. 例如:无論把一个多項式在复数域内分解还是利用符号添加来分解,"在实質上",即除等价外,都将得出同一的結果.

特别,$f(x)$ 的每一根或零点都有一个出現在分解

$$f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$$

中确定的重数.

当且仅当 $f(x)$ 与 $f'(x)$ 在分裂域上有一个非常数的公因子时,有重根存在(§ 24). 然而 $f(x)$ 与 $f'(x)$ 在任意分裂域上的最大公因子与在 $\Delta[x]$ 中的一样(§ 21,习題 1). 因此,通过作出 $f(x)$ 与 $f'(x)$ 在 $\Delta[x]$ 中的最大公因子,就已經能够知道 $f(x)$ 在它的分裂域中是否有重根.

同一多項式的含在一个公共包括域 Ω 中的两个分裂域不仅等价,而且相等. 因为当在 Ω 中有两个分解

$$f(x) = (x-\alpha_1)\cdots(x-\alpha_n),$$

$$f(x) = (x-\bar{\alpha}_1)\cdots(x-\bar{\alpha}_n)$$

成立时，根据在 $\Omega[x]$ 中唯一因子分解定理，除次序外，因子是唯一确定的。

正规扩域. 一个域 Σ 說是在 Δ 上正規的，假如第一，它对于 Δ 是代数的；第二，$\Delta[x]$ 中每一在 Σ 內有一个零点 α 的不可約多項式 $g(x)$ 在 $\Sigma[x]$ 中完全分解成綫性因子[1]。

根据以下定理，我們所作的分裂域是正規的：

由 Δ 通过添加 $\Delta[x]$ 中一个或多个甚至无穷个多項式的全部零点所生成的域是正規的.

首先，我們可以把无穷多个多項式的情形归到有限的情形；因为这个域的每一元素 α 只依賴于有限多个多項式的根，并且对于以 α 为零点的不可約多項式的分解，我們可以完全限于这有限多个根所生成的域內。

进一步有限个多項式的情形又可以归到一个多項式的情形，为此我們把所有这些多項式相乘并且添加积的零点；这些元素就如同取一切因子的零点一样.

这样，設 $\Sigma=\Delta(\alpha_1,\cdots,\alpha_n)$，其中 α_ν 是一个多項式的零点，并且設 $\Delta[x]$ 的不可約多項式 $g(x)$ 在 Σ 中有一个零点 β. 当 $g(x)$ 在 Σ 中不完全分解时，我們可以添加 $g(x)$ 的另一零点 β' 而将 Σ 扩张为一个域 $\Sigma(\beta')$；于是，由于 β 与 β' 共軛，所以

$$\Delta(\beta)\cong\Delta(\beta').$$

---

1) 这个定义也可以如此叙述：一个代数扩张 Σ 是正規的，假如 Σ 在含有一个代数元素 α 的同时，也含有 α 的一切共軛元素(在任意包括域內). 在任意包括域內与 α 共軛的元素不外是以 α 为零点的同一不可約多項式 $g(x)$ 的根，并且这个包括域总可以如此选取，使得 $g(x)$ 在其中完全分解. 然而这个定义在此处将被避免，因为它涉及一切包括域的总体，看起来不太完美(撇开集合論中关于这个总体的疑难之点，这是可以适当避免的)，因为我們实际上只涉及 Σ 与 Δ 的一个性質.

在这个同构之下，Δ 的元素，从而多项式 $f(x)$ 的系数变为自身．現在对左右两端添加 $f(x)$ 的一切零点，于是可以将这个同构开拓成为

$$\Delta(\beta, \alpha_1, \cdots, \alpha_n) \cong \Delta(\beta', \alpha_1, \cdots, \alpha_n),$$

其中 α_i 仍变为 α_j，也許按另外的次序．现在 β 是 $\alpha_1, \cdots, \alpha_n$ 的一个有理函数，系数在 Δ 内：

$$\beta = r(\alpha_1, \cdots, \alpha_n),$$

并且这个有理关系在任何同构之下保持成立． 由此，β' 也是 $\alpha_1, \cdots, \alpha_n$ 的一个有理函数，从而也属于域 Σ，这与假定相违．

逆定理． Δ 上的一个正規扩域由添加一組多項式的一切零点所生成，并且当这个域是有限的时候，甚至是由添加一个多項式的一切零点所生成．

証明． 域 Σ 由添加代数元的集 $\mathfrak{M}$ 生成．（一般我們可以取，例如，$\mathfrak{M} = \Sigma$；在有限情形 $\mathfrak{M}$ 是有限的．）$\mathfrak{M}$ 中每一元素滿足一个系数在 Δ 中的代数方程 $f(x) = 0$，这个方程在 Σ 中完全分解．添加所有这些多項式的全部零点（相应地，当这样的多項式的个数有限时，添加它們积的全部零点）至少与单独添加 $\mathfrak{M}$ 所生成的域一样，这就是說，由此生成整个的域 Σ，証毕．

一个不可約方程 $f(x) = 0$ 叫做*正規的*，假如由添加它的*一个*根所生成的域已經正規，即 $f(x)$ 在其中完全分解．

方程 $f(x) = 0$ 的 Galois *豫解式*是具有以下性質的一个不可約方程 $g(x) = 0$，即添加这个方程的一个根就已經生成多項式 $f(x)$ 的完全分裂域．这种豫解式的存在将在以后（§ 43）証明．

习題． 1．設 $\Delta \subseteq \Sigma \subseteq \Omega$ 且 Ω 在 Δ 上是正規的，那末 Ω 在 Σ 上是正規的．

2．作出 $x^3 - 2$ 对于有理数域 Γ 的分裂域． 証明：若 α 是一个根，那末

$\Gamma(\alpha)$ 不正規.

3. 若 $f(x)$ 在域 $\mathbf{K}$ 中不可約，那末 $f(x)$ 在一个正規扩域中分解为对于 $\mathbf{K}$ 共軛的次数完全相同的因子.

4. 每一个对于 Δ 的二次扩域对于 Δ 都是正規的.

§39. 单 位 根

我們在前面已經闡述了域論的一般基础. 在进一步发展这个一般理論之前，我們將把所得的定理应用到某些完全特殊的方程及特殊的域上.

設 Π 是一个素域而 h 是一个对于 Π 的特征来説不与零同余的自然数. (如果特征是零，那末 h 是一个任意的自然数.) 所謂一个 h **次单位根**，我們理解为多項式

$$f(x) = x^h - 1$$

在任意扩域中的零点.

在一个域内的 h 次单位根对乘法来説作成一个 Abel 羣.

因为当 $\alpha^h = 1$ 及 $\beta^h = 1$ 时，也有 $(\alpha/\beta)^h = 1$，从而得出羣性質. 至于这个羣是 Abel 羣，显然.

羣元素 α 的阶是 h 的因子，因为必須有 $\alpha^h = 1$.

$f(x)$ 的分裂域 Σ 叫做**素域 Π 上的 h 次单位根域**. 多項式 $f(x)$ 分解成完全不同的綫性因子；这是因为 h 不能被域的特征整除，所以导数

$$f'(x) = hx^{h-1}$$

仅当 $x = 0$ 时才等于零，从而与 $f(x)$ 沒有公共零点. **所以在 Σ 中恰有 h 个 h 次单位根.**

我們現在把 h 分解成素因子：

$$h = \prod_{i=1}^{m} q_i^{\nu_i}.$$

在 h 次单位根的羣中，至多存在 h/q_i 个元素 a，使得 $a^{h/q_i}=1$；因为多项式 $x^{h/q_i}-1$ 至多有 h/q_i 个零点。因此在这个羣中存在一个元素 a_i 使得

$$a_i^{h/q_i} \neq 1.$$

羣元素

$$b_i = a_i^{h/q_i^{\nu_i}}$$

的阶是 $q_i^{\nu_i}$；因为它的 $q_i^{\nu_i}$ 次幂等于 1，所以它的阶必须是 $q_i^{\nu_i}$ 的一个因子；然而它的 $q_i^{\nu_i-1}$ 次幂不等于 1，所以它的阶不能是 $q_i^{\nu_i}$ 的眞因子。現在乘积

$$\zeta = \prod_1^m b_i$$

作为具有互素阶 $q_1^{\nu_1}, \cdots, q_m^{\nu_m}$ 的元素的乘积，恰好有阶

$$\prod_1^m q_i^{\nu_i} = h$$

(§10. 习题 1)。一个阶恰好是 h 的单位根叫做一个 h 次**原根**。

一个原根的幂 $1, \zeta, \zeta^2, \cdots, \zeta^{h-1}$ 都不相等，然而因为羣正好有 h 个元素，所以它的一切元素都是 ζ 的幂。由此得：

h 次单位根羣是循环羣，并且是由每一个原根 ζ 所生成的。

h 次原根的个数現在很容易确定。我們首先以 $\varphi(h)$ 表示。**$\varphi(h)$ 是在一个 h 阶循环羣中阶为 h 的元素的个数**[1]。首先設 h 是一个素数的幂，$h=q^\nu$，那末，ζ 的 q^ν 个幂中，除去 $q^{\nu-1}$ 个 ζ^q 的冪外，都是 h 阶元素；从而

$$\varphi(q^\nu) = q^\nu - q^{\nu-1} = q^{\nu-1}(q-1) = q^\nu\left(1-\frac{1}{q}\right). \tag{1}$$

---

1) 根据 §21，习题 4，$\varphi(h)$ 同时又是与 h 互素的 $\leqslant h$ 的自然数的个数。我們称 $\varphi(h)$ 为 Euler φ-函数。

其次，若 h 分解成两个互素的因子：$h=rs$，那末每一 h 阶的元素唯一地被表成一个 r 阶元素与一个 s 阶元素的乘积（§21，习题 3）；反过来，每一个这样的乘积都是一个 h 阶元素. r 阶元素属于由 ζ^s 所生成的 r 阶循环羣；从而它的个数是 $\varphi(r)$. 同样，s 阶元素的个数是 $\varphi(s)$；因此，对于乘积的个数，我們有

$$\varphi(h)=\varphi(r)\varphi(s).$$

如果象前面那样，h 分解为无公因子的素数冪：

$$h=\prod_1^m q_i^{\nu_i},$$

那末累次应用这个公式，由此推出

$$\varphi(h)=\varphi(q_1^{\nu_1}q_2^{\nu_2}\cdots q_m^{\nu_m})=\varphi(q_1^{\nu_1})\varphi(q_2^{\nu_2})\cdots\varphi(q_m^{\nu_m}),$$

于是由(1)：

$$\varphi(h)=q_1^{\nu_1-1}(q_1-1)q_2^{\nu_2-1}(q_2-1)\cdots q_m^{\nu_m-1}(q_m-1)$$

$$=h\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_m}\right).$$

这样

h 次原根的个数是

$$\varphi(h)=h\prod_1^m\left(1-\frac{1}{q_i}\right).$$

我們令 $n=\varphi(h)$. 設 h 次原根是 $\zeta_1,\cdots,\zeta_n$. 它們是多项式

$$(x-\zeta_1)(x-\zeta_2)\cdots(x-\zeta_n)=\Phi_h(x)$$

的零点. 我們有

$$x^h-1=\prod_{d\mid h}\Phi_d(x), \tag{2}$$

此处 d 遍历 h 的正因子[1]；因为每一个 h 次原根对于 h 的一个而且仅一个正因子 d 而言是 d 次原根，从而 x^h-1 的每一綫性因子出現在多項式 $\Phi_d(x)$ 中的一个而且仅一个之內.

公式(2)唯一确定 $\Phi_h(x)$。因为由这个公式首先推出

$$\Phi_1(x)=x-1,$$

如果对于一切 $d<h$，Φ_d 已知时，那末 Φ_h 由(2)通过除法被确定。

因为，根据除法算式，这个除法可以在变元 x 的整系数多項式环内实施，于是有：

每一 $\Phi_h(x)$ 都是一个整系数多項式并且不依賴于域 Π 的特征(只要 h 不被特征整除).

根据以后将要提到的理由，多項式 $\Phi_h(x)$ 叫做**分圓多項式**. 它的明显的有理公式可以利用“Mobius 函数” $\mu(n)$ 給出，这个函数如下定义：

$$\mu(n)=\begin{cases}0, & \text{当 } n \text{ 含有一个素因子的平方时},\\(-1)^\lambda, & \text{当 } n=p_1p_2\cdots p_\lambda(\text{即 } n \text{ 沒有平方因子})\text{时},\\1, & \text{当 } n=1 \text{ 时}\end{cases}$$

($p_1, p_2, \cdots, p_\lambda$ 是数 n 的互不相同的素因子). Mobius 函数具有以下重要性質：

$$\sum_{d|h}\mu(d)=\begin{cases}1 & \text{对于}\quad h=1,\\0 & \text{对于}\quad h>1.\end{cases}$$

証明如下：令 $h=q_1^{\nu_1}\cdots q_m^{\nu_m}$，展开乘积 $\prod\limits_1^m(1-z_i)$，然后令一切 z_i 等于 1. 乘积的項

$$(-1)^\lambda z_{i_1}z_{i_2}\cdots z_{i_\lambda}$$

恰好与 h 的不含平方的因子 $d=q_{i_1}q_{i_2}\cdots q_{i_\lambda}$ 对应，并且有

---

1) $a|b$ (讀作 a 整除 b)意味着：a 是 b 的因子.

$$(-1)^{\lambda}=\mu(d).$$

这样,令一切 $z_i=1$, 于是当 $m>0$(即 $h>1$)时:

$$0=\prod_{1}^{m}(1-1)=\sum_{d|h}\mu(d),$$

当 $h=1$ 时, 显然有 $\sum\limits_{d|h}\mu(d)=1$.

我們現在断言:

分圓多項式由

$$\Phi_h(x)=\prod_{d|h}(x^d-1)^{\mu(h/d)} \tag{3}$$

給出.

为了証明,只需指出右端函数满足方程(2), 从而

$$x^h-1=\prod_{d|h}\prod_{d'|d}(x^{d'}-1)^{\mu(d/d')}.$$

一个固定的 $x^{d'}-1$ 的指数是数 $\mu(d/d')$, 此处 d 是 h 的一个因子而是 d' 的一个倍数,即是一切 $\mu(\lambda)$, 此处 λ 是 h/d' 的因子. 这些指数的和一般来説等于零,仅当 $h/d'=1$ 时才有值 1. 于是右端的双重积中只有一个因子 x^h-1 被保留且有指数 1. 因此方程(2)被函数(3)满足.

例:

$$\begin{aligned}\Phi_{12}(x)&=(x^{12}-1)^{+1}(x^6-1)^{-1}(x^4-1)^{-1}(x^2-1)^{+1}\\&=(x^6+1)^{+1}(x^2+1)^{-1}=x^4-x^2+1;\\\Phi_{q^v}(x)&=(x^{q^v}-1)^{+1}(x^{q^{v-1}}-1)^{-1}\\&=1+x^{q^{v-1}}+x^{2q^{v-1}}+\cdots x^{(q-1)q^{v-1}}.\end{aligned}$$

对于每一素数 q.

多項式 $\Phi_h(x)$ 可以很容易分解;例如,对于特征 11,

$$\Phi_{12}(x)=x^4-x^2+1=(x^2-5x+1)(x^2+5x+1).$$

然而以后(§ 55)将看到, 在特征零的素域中, 多項式 $\Phi_h(x)$ 不可

約，从而 h 次原根是共軛的．在 § 27 中，由 Eisenstein 定理我們已經知道，对于一切素数 h 就是这个情形；对于 $\Phi_8 = x^4 + 1$ 及 $\Phi_{12} = x^4 - x^2 + 1$ 就是 § 27，习題 3 及 § 26，习題 5 的內容。

一个常常应用的定理如下：

若 ζ 是一个 h 次单位根，那末

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{h-1} = \begin{cases} h & (\zeta = 1) \\ 0 & (\zeta \neq 1). \end{cases}$$

証明由几何級数的和公式立刻得到：对于 $\zeta \neq 1$，我們得到

$$\frac{1 - \zeta^h}{1 - \zeta} = 0.$$

习題． 1．h 次单位根域对奇数 h 来說同时是 $2h$ 次单位根域．

2．三次及四次单位根域在有理数域上是二次的．把这些单位根表成平方根．

3．八次单位根域对于 Gauss 数域 $\Gamma(i)$ 是二次的．把一个八次原根用 $\Gamma(i)$ 中一个元素的平方根表示．

4．在特征 p 的情形，$(p^\lambda h)$ 次单位根同时是 h 次单位根．［这就辨明开始所作的限制 $h \not\equiv 0(p)$．］

5．"分圓方程" $\Phi_h(x) = 0$ 永远是正規的．

§ 40. Galois 域（有限域）

我們已經在特征 p 的素域里遇到过有限个元素的域．有限域根据它的发現者 Galois 的名字也叫做 Galois 域．我們首先研究它的一般性質．

設 Δ 是一个 Galois 域且 q 是它的元素的个数．

Δ 的特征不可能是零，否則在 Δ 內的素域已經有无穷多个元素．設 p 是 Δ 的特征．于是素域 Π 与整数模 p 的同余类环同构并且含有 p 个元素．

因为在 Δ 中只有有限个元素，所以在 Δ 中存在一个对于 Π 的

极大綫性无关元素組 $\alpha_1, \cdots, \alpha_n$. n 是域次数 $(\Delta:\Pi)$, 并且Δ的每一元素有形式

$$(1) \qquad c_1\alpha_1 + \cdots + c_n\alpha_n,$$

系数 c_i 是Π中唯一确定的元素.

对于每一系数 c_i 有 p 个可能的值; 因此恰好有 p^n 个形式如(1)的表示式. 因为它們表示域的全部元素,所以有

$$q = p^n.$$

于是証明了: 一个 Galois 域的元素的个数是它的特征 p 的冪, 而冪指数給出域次数 $(\Delta:\Pi)$.

每一个体除去零元素是一个乘法羣. 在 Galois 域的情形这个羣是一个 Abel 羣并且它的阶是 $q-1$. 任意元素 α 的阶一定是 $q-1$ 的一个因子;从而

$$\alpha^{q-1} = 1, \quad 对任意 \quad \alpha \neq 0.$$

由此推出的方程

$$\alpha^q - \alpha = 0$$

对于 $\alpha = 0$ 也成立. 因此域的一切元素都是函数 $x^q - x$ 的零点. 設 $\alpha_1, \cdots, \alpha_q$ 是域元素,那末 $x^q - x$ 必須能被

$$\prod_1^q (x - \alpha_i)$$

整除. 于是根据次数,

$$x^q - x = \prod_1^q (x - \alpha_i).$$

从而Δ是由添加函数 $x^q - x$ 的一切零点所生成的. 根据所述, Δ除同构外是唯一确定的(§ 38);因此

对于給定的 p 及 n, 一切具有 p^n 个元素的域都是同构的.

我們現在指出,对于每一 $n > 0$ 及每一 p, 的确存在一个含有

$q = p^n$ 个元素的域。

我們从特征 p 的素域 Π 出发，并且在 Π 上作一个域，在其中 $x^q - x$ 完全分解成綫性因子．在这个域內我們考慮 $x^q - x$ 的零点的集．这个集是一个域，因为根据 § 33，习題 1，由 $x^{p^n} = x$ 及 $y^{p^n} = y$ 推出：

$$(x - y)^{p^n} = x^{p^n} - y^{p^n},$$

并且当 $y \neq 0$ 时：

$$\left(\frac{x}{y}\right)^{p^n} = \frac{x^{p^n}}{y^{p^n}},$$

从而两个零点的差与商仍是零点．

多項式 $x^q - x$ 只有单零点；因为由于 $q \equiv 0(p)$，它的导数

$$qx^{q-1} - 1 = -1,$$

而 -1 不是零．因此它的零点的集是一个具有 q 个元素的域．

这样就証明了：

对于每一素数幂 $q = p^n (n > 0)$ 存在并且除同构外，只存在一个含有 q 个元素的 Galois 域．域的元素是 $x^q - x$ 的零点．

正好有 p^n 个元素的 Galois 域以后用 $GF(p^n)$ 表示。

令 $q-1 = h$ 并且注意到 Galois 域的一切非零元素都是 $x^h - 1$ 的零点，因而是 h 次单位根．由于 h 与 p 互素，所以对于这些单位根，前一节所說的一切都成立：

一切非零的域元素都是一个 h 次原根的冪．或者：Galois 域的乘法羣是一个循环羣．

这个定理完全揭露了有限域的构造．

$GF(p^n)$ 的一切子域很容易定出．每一个子域有一个次数 m，它是 n 的因子，因而含有 p^m 个元素，它們由以下事实所刻划，卽它們必須是 $x^{p^m} - x$ 的零点．然而对于 n 的每一正因子 m 也确

实存在一个这样的子域；因为当 m 是 n 的一个因子时，p^m-1 是 $p^n-1=(p^m-1)(p^{n-m}+p^{n-2m}+\cdots+p^m+1)$ 的因子，从而 $x^{p^m-1}-1$ 是 $x^{p^n-1}-1$ 的因子而 $x^{p^m}-x$ 是 $x^{p^n}-x$ 的因子。因为最后多项式在 $GF(p^n)$ 中完全分解，所以前者也必须如此，并且它的零点組成一个 $GF(p^m)$. 这就証明了：对 n 的每一因子 $m>0$，在 $GF(p^n)$ 中存在一个且只一个 m 次子域 $GF(p^m)$. 一个元素 $\alpha\neq 0$，当它满足方程 $\alpha^{p^m}-1=0$，从而它的阶（在乘法羣）是 p^m-1 的一个因子时，属于这个子域.

下一节我們将用到以下定理：

对于每一元素 a，一个特征 p 的 Galois 域恰好含有一个 p 次根.

証明. 对于每一元素 x，在域中存在一个 p 次冪 x^p. 由于

$$(x-y)^p=x^p-y^p,$$

不同的元素有不同的 p 次冪. 因此在域中 p 次冪的个数恰与元素的个数一样多. 所以一切元素都是 p 次冪.

最后我們还要定出域 $\Sigma=GF(p^m)$ 的自同构.

首先，$\alpha\to\alpha^p$ 是一个自同构. 因为一方面根据前面的定理，这个对应是可逆单值的；另一方面

$$(\alpha+\beta)^p=\alpha^p+\beta^p,$$

$$(\alpha\beta)^p=\alpha^p\beta^p.$$

这个自同构的冪将 α 映成 $\alpha^p,\alpha^{p^2},\cdots,\alpha^{p^m}=\alpha$. 这样，我們已經找到 m 个自同构.

在 § 41 中看到，不可能有多于 m 个自同构. 因此以上所定出的自同构是仅有的自同构.

对于 $n=1$ 的特殊情形，对 $GF(p^n)$ 成立的定理应用到同余类环 $C/(p)$ 上，就产生初等数論中所熟知的定理，即：

1. 一个关于 p 的同余式最多有和它次数一样多的模 p 的根。

2. Fermat 定理

$$a^{p-1}\equiv 1(p)\quad 对于\quad a\not\equiv 0(p).$$

3. 存在一个"模 p 的本原数 ζ"，使得对于任意与 p 无公因子的数 b 与 ζ 的一个幂模 p 同余.（或者：模 p 的同余类羣，除零类外，是循环羣.）

4. $GF(p^n)$ 中一切非零元素 $a_1, a_2, \cdots, a_h$ 的乘积是 -1，因为

$$x^h-1=\prod_1^h(x-a_\nu).$$

对于 $n=1$，我們得到"Wilson 定理"：

$$(p-1)!\equiv -1(p).$$

习题. 1. 設 α 是 $\Pi[x]$ 中一个 m 次多項式 $f(x)$ 在 $GF(p^n)$ 中的一个零点，那末 $f(x)$ 的全部零点（与 α 共軛的元素）由

$$\alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^m}=\alpha$$

給出。

2. 若 r 与 p^n-1 无公因子，那末 $GF(p^n)$ 的每一元素是一个 r 次冪. 若 r 是 p^n-1 的一个因子，那末 $GF(p^n)$ 中这样的元素而且只是这样的元素 α 才是 r 次冪，它們滿足方程

$$\alpha^{\frac{p^n-1}{r}}=1.$$

給出数論的特殊化（"r 次冪剩余"）！

3. 当交換环 $\mathfrak{o}$ 的一个素理想 $\mathfrak{p}$ 只有有限个同余类时，$\mathfrak{o}/\mathfrak{p}$ 是一个 Galois 域。

4. 特别在 Gauss 整数环中研究对于素理想 $(1+i)$, (3), $(2+i)$, (7) 的同余类环。

5. 給出 $GF(9)$ 中一个八次原根在 $GF(3)$ 中的不可約方程；同样給出在 $GF(8)$ 中一个七次原根在 $GF(2)$ 中的不可約方程。

6. 对于每一 p 及 m，存在模 p 不可約的整系数多項式 $f(x)$. 所有这些多項式都是 $x^{p^m}-x$ 的因子（模 p）.

Galois 域的一个有趣性質已經被 C. Chevalley 証明：*Abh. Math. Sem. Hamburg*, **11** (1935), 73.

§41. 可分与不可分扩张

設 Δ 是一个域.

我們問：一个在 $\Delta[x]$ 中不可約的多項式在一个扩域內能否有重零点？

$f(x)$ 有重零点，必須 $f(x)$ 与 $f'(x)$ 有一个非常数的公因子，根据 §38 它可以在 $\Delta[x]$ 中算出. 若 $f(x)$ 不可約，那末 $f(x)$ 与一个低次多項式不可能有非常数公因子；因此必須 $f'(x)=0$.

令

$$f(x)=\sum_{0}^{n} a_\nu x^\nu,$$

$$f'(x)=\sum_{1}^{n} \nu a_\nu x^{\nu-1}.$$

如果 $f'(x)=0$，那末每一系数必須等于零：

$$\nu a_\nu = 0 \quad (\nu = 1, 2, \cdots).$$

在特征零的情形，由此推出 $a_\nu=0$ 对一切 $\nu\neq 0$. 因而一个非常数多項式不可能有重零点. 在特征 p 的情形，对于 $a_\nu\neq 0$ 也可能 $\nu a_\nu=0$；然而这时必須

$$\nu\equiv 0(p).$$

这样，$f(x)$ 若有一个重零点，除去具有 $\nu\equiv 0(p)$ 的項 $a_\nu x^\nu$ 外，一切項都应該等于零；从而 $f(x)$ 有形式

$$f(x)=a_0+a_p x^p+a_{2p}x^{2p}+\cdots.$$

反过来：当 $f(x)$ 有这样形式时，$f'(x)=0$.

在这一情形我們可以写

$$f(x)=\varphi(x^p).$$

这样就証明了：对于特征零，一个在 $\Delta[x]$ 中不可約的多項式 $f(x)$ 只有单零点；对于特征 p，$f(x)$（假設它不是常数）有重零点，当且仅当 $f(x)$ 可以写成 x^p 的函数时。

在后一情形，$\varphi(x)$ 本身也可能是 x^p 的函数。这时 $f(x)$ 是 x^{p^2} 的函数。設 $f(x)$ 是 x^{p^e} 的函数：

$$f(x) = \psi(x^{p^e}),$$

但不是 $x^{p^{e+1}}$ 的函数。$\psi(y)$ 自然不可約。再者，$\psi'(y) \neq 0$；否則将有 $\psi(y) = \chi(y^p)$，从而 $f(x) = \chi(x^{p^{e+1}})$，与假設相违。因此 $\psi(y)$ 只有单零点。

我們在一个扩域中分解 $\psi(y)$ 为綫性因子：

$$\psi(y) = \prod_1^m (y - \beta_i).$$

由此得

$$f(x) = \prod_1^m (x^{p^e} - \beta_i).$$

設 α_i 是 $x^{p^e} - \beta_i$ 的一个零点。那末有

$$\alpha_i^{p^e} = \beta_i,$$

$$x^{p^e} - \beta_i = x^{p^e} - \alpha_i^{p^e} = (x - \alpha_i)^{p^e}.$$

因而 α_i 是 $x^{p^e} - \beta_i$ 的一个 p^e 重零点，并且

$$f(x) = \prod_1^m (x - \alpha_i)^{p^e}.$$

所以 $f(x)$ 的全部零点都有同一重数 p^e。

多項式 ψ 的次数 m 叫做 $f(x)$ 的（或 α_i 的）簡約次数；e 叫做 $f(x)$（或 α_i）对于 Δ 的指数。在次数，簡約次数及指数之間关系

$$n = mp^e$$

成立。m 同时又是 $f(x)$ 的不同零点的个数。

如果ϑ是一个在$\Delta[x]$中不可約且具有完全分离(单)零点的多項式的零点，那末就称ϑ是对于Δ可分的或第一种的[1]. 不可約多項式$f(x)$，当它的零点都是可分的时候，也叫做可分的. 在相反的情形就称代数元 ϑ 或不可約多項式 $f(x)$ 为不可分的或第二种的. 最后，一个代数扩域Σ，当它的元素全部是对于Δ可分的时候，就叫做对于Δ可分的，而其他每一代数扩域就叫做不可分的.

在特征零的情形，根据上述，每一不可約多項式(从而每一代数扩域)是可分的；在特征p的情形只有指数$e=0$的多項式(从而簡約次数$m=n$)才是可分的. 在特征 p 的情形，一个不可約非常数多項式$\varphi(x)$是不可分的，当且仅当它可以写成x^p的多項式.

我們以后将要看到，多数重要且有兴趣的扩域都是可分的，并且存在很大的一类域，它們沒有任何不可分扩张(所謂"完全域"). 基于这个理由，以下特别与不可分扩张有关的一切討論都用小字书写.

我們現在考虑代数域$\Sigma=\Delta(\vartheta)$. 当定义方程$f(x)=0$的次数n同时表示域次数$(\Sigma:\Delta)$时，約簡次数m同时就表示在以下精确规定的意义下域Σ的同构的个数：我們只考虑这样的同构$\Sigma\cong\Sigma'$，它使得子域Δ的一切元素不动，从而Σ被映成一个等价的域Σ'("Σ对于Δ的相对同构")，并且只考虑这样的同构，在这个同构之下象域Σ'与Σ同在一个适当选取的包括域Ω内. 以下定理成立：

适当地选取包括域Ω，$\Sigma=\Delta(\vartheta)$恰好有m个相对同构，并且选不出任何Ω使得Σ有多于m个这样的同构.

---

1) "第一种的"这一說法起源于 Steinitz. 我附加"可分的"一詞，这在表示$f(x)$的一切零点都是分离的时候更有启发性.

証明． 每一相对同构必定把 ϑ 映成一个在 Ω 中的共軛元 ϑ'. 现在如此选取 Ω，使得 $f(x)$ 在 Ω 中完全分解成綫性因子，于是 ϑ 确实有 m 个共軛元素 $\vartheta, \vartheta' \cdots$. 然而不論 Ω 怎样选择，ϑ 不可能有多于 m 个共軛元. 现在注意，相对同构 $\Delta(\vartheta) \cong \Delta(\vartheta')$ 由 $\vartheta \to \vartheta'$ 的給出而完全确定. 因为若 ϑ 映成 ϑ' 而 Δ 的每一元素保持不动，那末必定

$$\Sigma a_k \vartheta^k \qquad (a_k \in \Delta)$$

映成

$$\Sigma a_k \vartheta'^k,$$

并且这就确定了这个同构.

特别若 ϑ 是可分的，那末 $m = n$，从而相对同构的个数等于域次数.

以后当說到 $\Sigma = \Delta(\vartheta)$ 的（相对）同构，ϑ 的共軛或 Σ 的共軛域（对于 Δ）时，我們永远分别理解为同构或共軛是在一个适当选择的域 Ω 內，这个域，正如上面那样，总可以选取 $f(x)$ 的分裂域，即 Δ 上包含 Σ 的最小正規扩域.

当我們有一个扩域，在其中每一个方程 $f(x) = 0$ 都完全分解成綫性因子时（如同在复数域中那样），那末可以一次选取这个固定域作为 Ω，而在說到同构时总可以略去"在 Ω 內"一詞. 在数域的理論中就常常这样作. 在 § 62 里我們将指出对于抽象域来說也可以提供这样的 Ω.

习题． 1. 設 Π 是一个特征 p 的素域而 x 是一个不定元，那末方程 $z^p - x = 0$ 在 $\Pi(x)[z]$ 中不可約并且由这个方程所定义的域 $\Pi(x^{1/p})$ 在 $\Pi(x)$ 上不可分.

2. 作出下列域对于有理数域 Γ 的相对同构：

a) 五次单位根域；

b) 域 $\Gamma(\sqrt[3]{2})$.

3. 若 $\vartheta^{p^e}=\gamma$ 属于 Δ 而 $\vartheta^{p^{e-1}}$ 不属于 Δ，那末多项式 $x^{p^e}-\gamma$ 在 $\Delta[x]$ 中不可約. [为了証明，指出 ϑ 在 Δ 上的次数正好是 p^e.]

上面定理的一个推广如下:

設一个扩域 Σ 是由 Δ 通过逐次添加 m 个代数元 $\alpha_1, \cdots, \alpha_m$ 而生成的，又設每一 α_i 是一个具有簡約次数 n_i' 的在 $\Delta(\alpha_1, \cdots, \alpha_{i-1})$ 內不可約方程的根，那末在一个适当选取的包括域 Ω 內，Σ 刚好有 $\prod_1^m n_i'$ 个对于 Δ 的相对同构，并且不能在任何包括域內有多于 m 个这样的同构.

証明. 这个定理对于 $m=1$ 来說已經被証明. 于是可以认为定理对于 $\Sigma_1=\Delta(\alpha_1, \cdots, \alpha_{m-1})$ 已經正确: 在一个适当选取的 Ω_1 內恰好有 Σ_1 的 $\prod_1^{m-1} n_i'$ 个相对同构并且不能再多. 令这 $\prod_1^{m-1} n_i'$ 个同构之一是 $\Sigma_1 \to \bar{\Sigma}_1$. 我們現在断言，这个同构在一个适当的 Ω 內恰好有 n_m' 种方法开拓为同构 $\Sigma=\Sigma_1(\alpha_m) \cong \bar{\Sigma}=\bar{\Sigma}_1(\bar{\alpha}_m)$ 并且不能多于 n_m' 种方法.

α_m 在 Σ_1 中滿足一个恰好有 n_m' 个不同的根的方程 $f_1(x)=0$. 在同构 $\Sigma_1 \to \bar{\Sigma}_1$ 之下令 $f(x)$ 映成 $\bar{f}_1(x)$. 那末 $\bar{f}_1(x)$ 在一个适当的扩域內仍有 n_m' 个不同的根并且不能再多. 令 $\bar{\alpha}_m$ 是这样的一个根. 随着 $\bar{\alpha}_m$ 的选取，同构 $\Sigma_1 \cong \bar{\Sigma}_1$ 可以用一种而且只一种方法开拓成一个同构 $\Sigma_1(\alpha_m) \cong \bar{\Sigma}_1(\bar{\alpha}_m)$ 且 $\alpha_m \to \bar{\alpha}_m$: 这个开拓由公式

$$\Sigma c_k \alpha_m^k \to \Sigma \bar{c}_k \bar{\alpha}_m^k$$

給出. 因为我們可以有 n_m' 种方法选取 α_m，所以对于每一个取定的同构 $\Sigma_1 \to \bar{\Sigma}_1$，存在 n_m' 个这样的开拓. 由于这个同构本身可以有 $\prod_1^{m-1} n_i'$ 种方法选取，所以对于 Σ 一共有(在这样的一个包括域 Ω 內，在其中所考虑的一切方程都完全分解)

$$\prod_1^{m-1} n_i' \cdot n_m' = \prod_1^m n_i'$$

个相对同构并且不能再多，証毕.

若 n_i 是 α_i 对于 $\Delta(\alpha_1, \cdots, \alpha_{i-1})$ 的全(非簡約)次数，那末 n_i 同时是 $\Delta(\alpha_1, \cdots, \alpha_i)$ 对于 $\Delta(\alpha_1, \cdots, \alpha_{i-1})$ 的域次数; 从而域次数 $(\Sigma:\Delta)$ 等于 $\prod_1^m n_i$. 比較这个个数与同构的个数，于是得到:

一个有限扩域 $\Sigma=\Delta(\alpha_1, \cdots, \alpha_m)$ 对于 Δ 的相对同构的个数(在一个

适当的扩域Ω内)，当且仅当每一α_i对于相应的域$\Delta(\alpha_1, \cdots, \alpha_{i-1})$是可分的时候，等于域次数$(\Sigma:\Delta)$. 反过来，只要有一个$\alpha_i$不可分，那末同构的个数就小于域次数。

由这个定理立刻推出一些重要的推論. 首先这个定理說明，每一个α_i对于前一个域的可分性是一个域的性質而不依賴于生成元α_i的选择. 因为这个域的任意一个元素β都可以选作第一个生成元，所以立刻推出，只要一切α_i在所說的意义下是可分的，那末Σ的每一元素β是可分的. 从而：

若对于Δ逐次添加元素$\alpha_1, \cdots, \alpha_n$并且若每一$\alpha_i$对于前一个域是可分的，那末所生成的域

$$\Sigma = \Delta(\alpha_1, \cdots, \alpha_n)$$

对于Δ是可分的.

特别：可分元素的和、差、积、商都是可分的.

再者：若β对于Σ可分而Σ对于Δ可分，那末β对于Δ可分. 因为β满足一个带有有限个属于Σ的系数$\alpha_1, \cdots, \alpha_m$的方程，所以对于$\Delta(\alpha_1, \cdots, \alpha_m)$可分。从而

$$\Delta(\alpha_1, \cdots, \alpha_m, \beta)$$

可分。

最后，我們有：Δ的一个可分有限扩域Σ的相对同构的个数等于域次数$(\Sigma:\Delta)$.

因为根据上述，对于可分元素施上一切有理运算仍旧得到可分元素，所以在Δ的一个任意扩域中可分元素本身作成一个域Ω_0. 我們也可以把Ω_0記作Δ在Ω中的最大可分扩域。

若Ω对于Δ是代数的，然而不一定可分，那末Ω中每一元素α的p^e次冪在Ω_0内，此处e是这个元素的指数. 由本节开始的考慮，立刻推出，α^{p^e}满足一个具有完全不同的根的方程。于是：

Ω由Ω_0通过开p^e次方生成。

特别，若Ω对于Δ是有限的，那末指数e自然有界. 这些指数中的最大者，仍旧記作e，叫做Ω的指数. Ω_0的次数叫做Ω的簡約次数.

开p^e次方自然也可以通过依次开p次方而达到. 在开p次方时，如果这个方根已經不在域内（即在添加一个不可約方程$x^p - \beta = 0$的根时），那末域次数就乘以p. 于是，当一个p次根已經开f次方时，我們最后将有

$$(\Omega:\Delta) = (\Omega_0:\Delta)\cdot p^f,$$

或者如同单純不可分扩張那样

$$\text{次数} = \text{簡約次数} \cdot p^f.$$

对于 p^e 次根的运算特別簡单. 若 α 是 β 的一个 p^e 次根,正如我們已經看到的那样,

$$x^{p^e} - \beta = x^{p^e} - \alpha^{p^e} = (x - \alpha)^{p^e};$$

因此,β 的一个 p^e 次根在它所存在的每一个域内是唯一确定的. 再者

$$\sqrt[p^e]{\alpha + \beta} = \sqrt[p^e]{\alpha} + \sqrt[p^e]{\beta},$$

$$\sqrt[p^e]{\alpha\beta} = \sqrt[p^e]{\alpha} \cdot \sqrt[p^e]{\beta},$$

这由自乘 p^e 次方就可以看出.

习題. 4. 設对于一个有限不可分扩张,e 与 f 如上定义,那末 $e \leqslant f$. 在单純扩张时 $e = f$. 給出一个关于 $e < f$ 的例子. [添加两个或多个不定元的 p 次根.]

§ 42. 完全域及不完全域

一个域 Δ 叫做完全的,假如 $\Delta[x]$ 中每一个不可約多項式 $f(x)$ 都是可分的. 任何其他域都叫做不完全的.

以下两个定理表明,一个域在什么时候是完全的:

I. 特征零的域永远是完全的.

証明. 見 § 41.

II. 一个特征 p 的域是完全的,当且仅当对于每一元素来說,在域内存在一个 p 次根.

証明. 如果对于每一元素来說,在域内存在一个 p 次根,那末每一个只含有 x^p 的冪的多項式 $f(x)$ 都是一个 p 次冪,因为

$$f(x) = \sum_k a_k (x^p)^k = \{\Sigma \sqrt[p]{a_k}\, x^k\}^p;$$

这就是說,在这一情形,每一个不可約多項式都是可分的,从而域是可分的.

另一方面，如果在域内存在一个元素 α，它不是 p 次幂，那末考虑多项式

$$f(x) = x^p - \alpha.$$

設 $\varphi(x)$ 是 $f(x)$ 的一个不可約因子．添加 $\sqrt[p]{\alpha} = \beta$ 后，$f(x)$ 分解成完全相同的綫性因子 $(x - \beta)$，于是 $\varphi(x)$，作为 $f(x)$ 的因子，同时是 $(x-\beta)$ 的一个幂．若 $\varphi(x)$ 是綫性的，那末 $\varphi(x) = x-\beta$ 而 β 将属于域 Δ，与假定相违．所以 $\varphi(x) = (x - \beta)^k$，$k > 1$，是 Δ 上的一个不可分多項式，从而 Δ 是一个不完全域．此外，根据 § 41，$\varphi(x)$ 的次数必須能被 p 整除，所以这时等于 p，即 $\varphi(x) = f(x)$．

由 II 及 § 40 的最后定理立即推出：

一切 Galois 域都是完全的．

在一个代数封閉域（定义在 § 62）中，每一个不可約多項式都是綫性的；从而

一切代数封閉域都是完全的．

由完全域的定义立刻推出下列两个定理：

一个完全域的每一代数扩张对于这个域是可分的．

对于每一不完全域来說，存在它的不可分扩张．

这个不可分扩张由添加一个第二种素多項式的任意一个零点而得到．

由 II 的証明中所作的注意，在一个特征 p 的完全域里，每一个只与 x^p 有关的多項式 $f(x)$ 都是一个 p 次幂；根据它的証明，对于多元多項式 $f(x, y, z, \cdots)$ 同时又是 x^p, y^p, z^p, $\cdots$ 的多項式的情形也成立．这也是特征 p 的完全域的一个常用到的性质．

习题． 1．一个完全域的每一个代数扩张都是完全的．

§ 43. 代数扩张的单純性. 本原元素定理

我們將研究在什么情形下域Δ的一个有限扩张是单純的，即由添加一个单独的生成元或"本原"元素生成的. 以下的本原元素定理在一类广泛的情形給出这个問題的答案. 这个定理是說:

設 $\Delta(\alpha_1, \cdots, \alpha_h)$ 是Δ的一个有限代数扩域而 $\alpha_2, \cdots, \alpha_h$ 是可分元素[1]. 那末 $\Delta(\alpha_1, \cdots, \alpha_h)$ 是一个单純扩张:

$$\Delta(\alpha_1, \cdots, \alpha_h) = \Delta(\vartheta).$$

証明. 我們首先对两个元素 α, β 其中至少 β 是可分的情形来証明这个定理. 設 $f(x) = 0$ 是对于 α 的不可約方程, $g(x) = 0$ 是对于 β 的不可約方程. 我們取一个域, 在其中 $f(x)$ 与 $g(x)$ 完全分解. 令 $\alpha_1, \cdots, \alpha_r$ 是 $f(x)$ 的不同的零点; $\beta_1, \cdots, \beta_s$ 是 $g(x)$ 的不同的零点;例如設 $\alpha_1 = \alpha$, $\beta_1 = \beta$.

我們可以假定Δ有无穷多个元素; 否則 $\Delta(\alpha, \beta)$ 也只有有限个元素, 而对于有限域来說本原元素的存在(甚至是一个原根, 除零元外域的一切元素都是它的冪)已經在 § 40 被証明.

对于 $k \neq 1$, 我們有 $\beta_k \neq \beta_1$, 于是方程

$$\alpha_i + x\beta_k = \alpha_1 + x\beta_1$$

对于每一 i 及每一 $k \neq 1$ 至多有一个根 x 在Δ內. 現在选取 c 不等于所有这些綫性方程的根, 那末对于每一 i 及 $k \neq 1$:

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1.$$

令

$$\vartheta = \alpha_1 + c\beta_1 = \alpha + c\beta.$$

于是 ϑ 是 $\Delta(\alpha, \beta)$ 的一个元素. 我們断言, ϑ 已經具有所要求的本原元素的性質: $\Delta(\alpha, \beta) = \Delta(\vartheta)$.

---

1) 即使 α_1 可分, 从而整个的域是可分时也沒有关系.

元素 β 満足方程

$$g(\beta)=0,$$

$$f(\vartheta-c\beta)=f(\alpha)=0,$$

系数在 $\Delta(\vartheta)$ 内。 多項式 $g(x)$, $f(\vartheta-cx)$ 只有公根 β;因为对于第一个方程的其他的根 $\beta_k(k\neq 1)$

$$\vartheta-c\beta_k\neq\alpha_i \qquad (i=1,\cdots,r),$$

从而

$$f(\vartheta-c\beta_k)\neq 0.$$

β 是 $g(x)$ 的单根；所以 $g(x)$ 与 $f(\vartheta-cx)$ 只有一个綫性因子 $x-\beta$ 公共。 这个最大公因子的系数必定在 $\Delta(\vartheta)$ 内；所以 β 在 $\Delta(\vartheta)$ 内。

这样，我們的定理对于 $h=2$ 被証明。 假定定理对于 $h-1$ $(\geqslant 2)$ 已証，于是有

$$\Delta(\alpha_1,\cdots,\alpha_{h-1})=\Delta(\eta),$$

于是由定理的已被証明的部分得出

$$\Delta(\alpha_1,\cdots,\alpha_h)=\Delta(\eta,\alpha_h)=\Delta(\vartheta);$$

从而定理对 h 也成立。

推論. 每一可分有限扩张是单純的。

这个定理大大地簡化了有限可分扩张的研究，因为借助于一目了然的基表达式

$$\sum_0^{n-1}a_k\vartheta^k,$$

这个扩张的构造及同构都很容易掌握。 作为例子，我們现在对于在 § 41 (小体字) 中利用同构的逐次开拓所証明的事实，即 Δ 的一个有限可分扩张 Σ 对于 Δ 的相对同构的个数等于次数 $(\Sigma:\Delta)$，又給出一个新的証明。 因为对于单純可分扩张来說，在 § 41 已被証

明，而每一个有限可分扩张，如现在所知，是单純的。

在特征零的情形每一有限扩张都是可分的，因而是单純的。然而就是在特征 p 的情形，我們也可以确切地指出一个有限扩张在什么时候是单純的：

一个特征 p 的域 Δ 的有限扩域 Σ 是单純的，当且仅当

$$n = mp^e, \tag{1}$$

此处 n 是扩域的次数，m 是簡約次数，e 是指数。

証明. 首先注意，若 $\Sigma = \Delta(\alpha_1, \cdots, \alpha_r)$，那末 Σ 的指数等于 $\alpha_1, \cdots, \alpha_r$ 的指数中最大值 e. 因为首先，Σ 的指数确实 $\geqslant e$. 然而 Σ 中一切元素都由 $\alpha_1, \cdots, \alpha_r$ 有理地表示（系数在 Δ 內），所以根据指数規則，Σ 中元素的 p^e 次冪可以由 $\alpha_1^{p^e}, \cdots, \alpha_r^{p^e}$ 有理地表示；从而这些 p^e 次冪是可分元素，而 Σ 的指数正好是 e. 根据 § 41，Σ 的可分元素作成一个在 Σ 內的可分扩域 Σ_0.

現在設 Σ 是单純的：$\Sigma = \Delta(\vartheta)$. 于是 $\vartheta^{p^e} \in \Sigma_0$. 这样，如果再令 $(\Sigma:\Sigma_0) = p^f$，那末 $f \leqslant e$ 并且（一般）$e \leqslant f$，从而 $e = f$；由此及 $n = mp^f$ 推出关系(1).

反过来設 (1) 成立. Σ_0 是一个有限可分扩张，因而是单純的：

$$\Sigma_0 = \Delta(\alpha).$$

我們求出 Σ 的一个元素 β，它正好有指数 e. 于是

$$\beta^{p^e} = \mu_0 \in \Sigma_0,$$

且 $x^{p^e} - \mu_0$ 在 Σ_0 中不可約，因为不然的話，$\beta^{p^{e-1}}$ 必須已經属于 Σ_0（§ 41，习題 3）. 因此 $\Sigma_0(\beta)$ 对于 Σ_0 有次数 p^e，从而对于 Δ 有次数 $n = mp^e$. 由于 Σ 对于 Δ 也有次数 n，所以 $\Sigma_0(\beta) = \Sigma$ 或 $\Sigma = \Delta(\alpha, \beta)$. 因为 α 是可分的，所以由本原元素定理得出，Σ 是单純的，証毕.

习題. 1. 若 x 及 y 都是不定元，那末 $\Delta(x, y)$ 的扩张 $\Delta(x^{1/p}, y^{1/p})$ 不再是单純的.

2. 对于特征 $\neq 2$ 及不定元 x, y，等式

$$\Delta(\sqrt{x}, \sqrt{y}) = \Delta(x, y, \sqrt{x} + \sqrt{y})$$

永远成立，然而对于特征 2 不成立.

§ 44. 范数与迹

首先設 Σ 是 Δ 的一个有限扩域. 把 Σ 映成它的共軛域的 Σ 的

相对同构把Σ的每一元素η也映成与η共軛的元素．为了簡单起見，我們假定Σ是一个单純扩域：$\Sigma=\Delta(\vartheta)$，于是

$$\eta=\psi(\vartheta)=a_0+a_1\vartheta+\cdots+a_{n-1}\vartheta^{n-1},$$

并且在同构之下，将ϑ代以它的共軛元素，就得到

$$\eta_\nu=\psi(\vartheta_\nu)=a_0+a_1\vartheta_\nu+\cdots+a_{n-1}\vartheta_\nu^{n-1}.$$

在这里将共軛元素ϑ_ν由1到n編号并且每一个出現在以ϑ为根的$\Delta[t]$中不可約多項式$\varphi(t)$的綫性因子分解中几次就賦予几个号碼．这样，对于可分的ϑ，每一同构算作一次，而对于不可分的ϑ，每一同构算作多次．自然η本身也出現在共軛元素之中．

我們現在考虑$\eta_1,\cdots,\eta_n$的初等对称函数，特别把和叫做η的迹：

$$\sum_{\nu=1}^{n}\eta_\nu=S(\eta)$$

而积叫做η的范数：

$$\prod_{\nu=1}^{n}\eta_\nu=N(\eta).$$

范数与迹显然都是基域Δ的元素．

我們把范数与迹的形成扩充到系数在Σ內的多項式上，在这里約定，同构$\vartheta\to\vartheta_\nu$只对这些多項式的系数起作用而不定元則保持不动．例如

$$N(z-\eta)=\prod_{\nu=1}^{n}(z-\eta_\nu). \tag{1}$$

多項式$G(z)=N(z-\eta)$的系数恰好就是$\eta_1,\cdots,\eta_n$的初等对称函数．因此只要有范数的概念就完全够了：迹以及其余的初等对称函数可以用范数$N(z-\eta)$来定义．

以上所給出的，在代数数論中常用的范数定义有一个优点，就

是范数和迹的两个基本性質

$$(2)\qquad \begin{cases} N(\alpha\beta)=N(\alpha)N(\beta)\\ S(\alpha+\beta)=S(\alpha)+S(\beta)\end{cases}$$

是自明的. 然而这个定义也有一个缺点,就是它不能推广到体或其它的代数上. 因此我們在以下給出范数的另外两个更适合于一般化的定义.

設 Σ 是域 Δ 上的一个具有限綫性秩 n 的体:

$$(\Sigma:\Delta)=n.$$

Δ 在 Σ 的中心內. Σ 的一个元素 η 的极小多項式指的是以 η 为零点的最低次(不可約)多項式:

$$(3)\qquad g(z)=z^m+b_1z^{m-1}+\cdots+b_m.$$

这个多項式的次数就是域次数

$$(\Delta(\eta):\Delta)=m.$$

为了得到一个 n 次多項式,我們令

$$(4)\qquad r=\frac{n}{m}=(\Sigma:\Delta(\eta)),$$

并且作出

$$(5)\qquad G(z)=g(z)^r=z^n+c_1z^{n-1}+\cdots+c_n$$

其中

$$c_1=rb_1,\quad c_n=b_m^r.$$

現在这个多項式的系数交替变号地代替先前的初等对称多項式的地位. 因此我們令

$$(6)\qquad S(\eta)=-c_1=-rb_1,$$

$$(7)\qquad N(\eta)=(-1)^nc_n=(-1)^{rm}b_m^r.$$

我們現在証明, 在 Σ 是一个域的情形这个新定义与旧定义一致. 为了証明这一点,只要多項式 (5) 与先前所定义的 $N(z-\eta)$

一致：

$$G(z) = N(z - \eta)$$

或

(8) $$g(z)^r = \prod_1^n (z - \eta_\nu)$$

就够了.

把右端多項式分解成不可約因子 $h_1(z)\,h_2(z)\cdots$. 每一个因子以某些 η_ν 为零点. 然而因为所有 η_ν 都与 η 共軛并且共軛元素滿足同一个不可約多項式，所以一切 $h_i(z)$ 除常数因子外必須与 $g(z)$ 一致. 因此(8)式右端的乘积除常数因子外是 $g(z)$ 的一个冪. 比較次数，于是看出这个冪指数只能是 r. 比較最高冪 $z^{rm} = z^n$ 的系数，我們看出，这个常数因子是 1. 于是(8)被証明.

这样，在交換的情形，范数与迹的这个新定义与旧定义一致. 然而不能說明，在体的情形范数与迹的这个新定义也具有性質(2). 因此我們再給出第三个等价的范数定义，这个定义除此之外还有一个优点，就是在任意代数中仍然有意义.

設 $(\omega_1, \cdots, \omega_n)$ 是 Δ 上代数 Σ 的一組基. 我們把所有乘积 $\eta\omega_j$ 由这組基綫性表示：

(9) $$\eta\omega_j = \sum_k c_{jk}\omega_k$$

并且作系数 c_{jk} 的行列式. 这个行列式 D 叫做 η 的**正則范数**.

首先証明，D 不依賴于基的选取. 設 $(\omega_1', \cdots, \omega_n')$ 是另一組基且

(10) $$\omega_i' = \sum_j a_{ij}\omega_j,$$

(11) $$\omega_k = \sum_l b_{kl}\omega_l',$$

那末由(9),(10)及(11)看出

$$\eta\omega_i' = \sum_j \sum_k \sum_l a_{ij}c_{jk}b_{kl}\omega_l',$$

所以这个新系数由

$$c_{il}' = \sum_j \sum_k a_{ij}c_{jk}b_{kl}$$

給出. 从而根据行列式的乘法定理推出对于元素 c_{ij}', a_{ij}, b_{kl} 的行列式 D', A, B 的方程

(12) $$D' = ABD.$$

另一方面,变换(10)与(11)是互逆的. 把(11)代入(10)并且比較左右两端的系数,于是看出,矩陣(a_{ij})与(b_{kl})的乘积是单位矩陣. 由此得

(13) $$1 = AB.$$

由(12)与(13)推出 $D' = D$: 正则范数 D 确实不依賴于基的选取.

現在特别設 Σ 是一个体. 我們問,当 Σ 换成一个包含它的代数 Ω 时,行列式 D 的情形怎样. 設$(\sigma_1, \cdots, \sigma_n)$是 Σ 在 Δ 上的一組基而$(\omega_1, \cdots, \omega_s)$是 Ω 在 Σ 上的一組基,那末$(\sigma_1\omega_1, \sigma_2\omega_1, \cdots, \sigma_n\omega_1, \cdots, \sigma_1\omega_s, \cdots, \sigma_n\omega_s)$是 Ω 在 Δ 上的一組基. Σ 的一个元素 η 的行列式 D_Σ 将由

$$\eta\sigma_j = \sum_k c_{jk}\sigma_k$$

求出. 用 ω_l 乘这些公式,由此得

(14) $$\eta\sigma_j\omega_l = \sum_k c_{jk}\sigma_k\omega_l.$$

因此右端的系数行列式 D_Ω 由 s 个相同的块(c_{jk})組成

$$
D = \left|\begin{array}{ccc}
\begin{array}{|ccc|} c_{11} & \cdots & c_{1n} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ c_{n1} & \cdots & c_{nn} \\ \hline \end{array} & 0 & \\
0 & \begin{array}{|ccc|} c_{11} & \cdots & c_{1n} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ c_{n1} & \cdots & c_{nn} \\ \hline \end{array} & \\
 & & \ddots
\end{array}\right|.
$$

于是在代数 Ω 中所作出的 η 的正则范数是

$$
(15) \qquad D_\Omega = D_\Sigma^s, \quad s = (\Omega : \Sigma).
$$

根据以上所述，我們可以証明，在体 Σ 的情形，正则范数 D_Σ 与先前所定义的范数 (7) 一致.

由公式 (15)，我們可以把元素 η 的正则范数 D_Σ 的計算限制在含 η 的最小体内，因而可以限制在域 $\Delta(\eta)$ 內，而 $(1, \eta, \eta^2, \cdots, \eta^{m-1})$ 是这个域的一組基. 关于这一組基，如果注意到定义方程 $g(\eta) = 0$，我們有

$$
\begin{gathered}
\eta \cdot 1 = \eta \\
\eta \cdot \eta = \eta^2 \\
\eta \cdot \eta^2 = \eta^3 \\
\cdots\cdots\cdots \\
\eta \cdot \eta^{m-1} = -b_m - b_{m-1}\eta - \cdots - b_1\eta^{m-1}.
\end{gathered}
$$

因此 η 在域 $\Delta(\eta)$ 內的行列式是

$$D_{\Delta(\eta)}=\begin{vmatrix}0 & 1 & 0 & \cdots\cdots & 0\\ 0 & 0 & 1 & \cdots\cdots & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & 0 & \cdots\cdots & 1\\ -b_m & -b_{m-1} & -b_{m-2} & \cdots & -b_1\end{vmatrix}=(-1)^m b_m.$$

于是由公式(15)推出

(16) $$D_\Sigma=D^r_{\Delta(\eta)}=(-1)^{mr}b^r_m,\quad r=(\Sigma:\Delta(\eta)).$$

比較(7)与(16)看出，D_Σ 确实是 η 在体 Σ 內的范数：

(17) $$N(\eta)=D_\Sigma.$$

如果 η 不是体元素，而是 $\Sigma[x_1, x_2, \cdots]$ 的一个多項式，那末同样的討論完全成立，只是必須設想不定元 $x_1, x_2, \cdots$ 添加到基本体上。当 η 本身是一个 h 次多項式时，范数 D_Σ 将是一个 nh 次多項式。例如，代替元素 η，我們考虑多項式 $z-\eta$，于是由(9)推出

$$(z-\eta)\omega_j=z\omega_j-\sum_k c_{jk}\omega_k,$$

(18) $$N(z-\eta)=\begin{vmatrix}z-c_{11} & -c_{12} & \cdots & -c_{1n}\\ -c_{21} & z-c_{22} & \cdots & -c_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ \cdots & \cdots & \cdots & \cdots\\ -c_{n1} & -c_{n2} & \cdots & z-c_{nn}\end{vmatrix}.$$

在 $N(z-\eta)$ 中 z^{n-1} 的系数取負号又是 η 的迹：

(19) $$S(\eta)=c_{11}+c_{22}+\cdots+c_{nn}.$$

我們現在对于任意代数通过(17)及(19)来定义(正則)范数与迹，并且証明，在这个定义的基础上公式(2)一般地成立。

設 $(\omega_1, \cdots, \omega_n)$ 是一組基而

(20) $$\alpha\omega_j=\sum_k a_{jk}\omega_k,$$

$$\beta\omega_j = \sum_k b_{jk}\omega_k. \tag{21}$$

用 α 乘(21)的左右两端并且应用(20)，于是得

$$\alpha\beta\omega_j = \sum_k \sum_l b_{jk}a_{kl}\omega_l.$$

因此属于 $\alpha\beta$ 的系数 c_{jl} 等于

$$c_{jl} = \sum_k b_{jk}a_{kl}.$$

由此根据行列式乘法定理推出

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

迹的关系更容易証明．由(20)与(21)相加得出

$$(\alpha+\beta)\omega_j = \sum_k (a_{jk}+b_{jk})\omega_k$$

$$S(\alpha+\beta) = \sum_j (a_{jj}+b_{jj}) =$$

$$= \sum_j a_{jj} + \sum_j b_{jj} = S(\alpha)+S(\beta).$$

习题． 1．在二次域 $\Delta(\sqrt{d})$ 中計算 $a+b\sqrt{d}$ 的范数．

2．設 Δ 是有理数域而 ϑ 满足不可約方程 $\vartheta^3+\vartheta+1=0$．在域 $\Delta(\vartheta)$ 中計算 $1+\vartheta^2$ 的范数．

在体和矩陣环里除了正則范数 $N(\eta)$ 以外还用到一个簡約范数 $n(\eta)$，而正則范数是它的一个冪．例如，在四元数体中，我們定义

$$n(a+bi+ck+dl) = a^2+b^2+c^2+d^2.$$

这个簡約范数的平方是正則范数

$$N(a+bi+ck+dl) = (a^2+b^2+c^2+d^2)^2.$$

在本书卷二最后一章里我們还将討論簡約范数与迹．

第六章　羣論續

內容.　在§§45和46中討論了羣概念的一种推广．§§47到49中給出了有关正規子羣和"合成羣列"的几个重要的普遍定理，而在§§50和51中則講解了有关置換羣的几个較特殊的定理，后者只在Galois理論中才用到．

§45. 带算子的羣

在这一节中我們要推广一下羣的概念，以便使得下面的各种討論具有更大的普遍性，这种普遍性对今后的各种应用（第十五章到第十七章）来說是非常必要的．仅对Galois理論感到兴趣的讀者可以暫时放过本节和下面紧接着的一节，并把以下各节中所遇到的羣（有限羣）理解为过去那种意义下的羣．

假設已經給定了：第一，（通常意义下的）一个羣$\mathfrak{G}$，其元素为$a, b, c, \cdots$；第二，某些称为算子的新对象$\eta, \Theta, \cdots$的集合Ω．其次，假設对每个算子Θ和羣中每个元素a定义了积Θa（算子Θ作用在元素a上），并且这个积仍属于羣$\mathfrak{G}$．再次，我們假設每个单独的算子Θ都是"可分配"的，即有

$$\Theta(ab) = \Theta a \cdot \Theta b. \tag{1}$$

換句話說，用算子Θ去"乘"$\mathfrak{G}$的元素，其效果是羣$\mathfrak{G}$的一个自同态[1]．如果所有这些条件都能滿足，我們就說$\mathfrak{G}$是一个带算子的

1）由此推出，用Θ去乘单位元素仍得单位元素，而用Θ去乘逆元素仍得逆元素．

羣，而 Ω 則称为**算子区**.

羣 $\mathfrak{G}$ 的一个(相对于算子区 Ω 来說的)**可許子羣**就是这样一个子羣 $\mathfrak{H}$，它在 Ω 中的算子的作用下不变，也就是說，如果 a 属于 $\mathfrak{H}$，則每个 Θa 也属于 $\mathfrak{H}$. 如果一个可許子羣同时是一个正規子羣，我們就說它是一个可許正規子羣.

例. 1. 如果以 $\mathfrak{G}$ 的全部內自同构为算子:

$$\Theta a = cac^{-1},$$

那末可許子羣就是那样一些子羣，它們在包含每个元素 a 的同时也包含着它的每个共軛元素 cac^{-1}，卽可許子羣是 $\mathfrak{G}$ 中的正規子羣.

2. 如果以 $\mathfrak{G}$ 的全部自同构为算子，那末可許子羣就是那样一些子羣，它們在每一个自同构之下变为其自身. 这样的子羣称为**特征子羣**.

3. 設 $\mathfrak{G}$ 是一个环，考慮它里面的加法，可以把它看成一个羣. 我們把这个环本身看成它的算子区 Ω，乘积 Θa 就是环中通常的乘积. 这样一来，条件 (1) 就是通常的分配律:

$$r(a+b) = ra + rb.$$

可許子羣就是环中的**左理想**，卽那样一些子羣，它們在包含每个元素 a 的同时也包含着所有的 ra.

4. 在有的場合下，把算子 Θ 写在羣元素的右边，卽把 Θa 改写成 $a\Theta$，要来得更加方便一些. 这时 (1) 就变成

$$(ab)\Theta = a\Theta \cdot b\Theta.$$

举例来說，如果我們把一个环 (作为加法羣看) 中的元素看成这样的右算子，而 $a\Theta$ 仍是环中通常的乘积，那末可許子羣就是环中的**右理想**.

5. 最后，我們可以把一部分算子写成左算子，另一部分算子写

成右算子．举例来說，如果我們在考虑一个环的加法羣时，以环中的元素作为算子，但每个元素既当作左乘因子也当作右乘因子看待，那末可許子羣就是环中的双边理想．

6．前面已經說过，一个模就是一个表成加羣形式的 Abel 羣．模也可以有一个算子区，称为模的乘子区．这时我們有

$$\Theta(a+b)=\Theta a+\Theta b.$$

在大部分場合下我們假定乘子区是一个环，并假定

$$(2)\qquad \begin{cases}(\eta+\Theta)a=\eta a+\Theta a,\\(\eta\Theta)a=\eta(\Theta a)\end{cases}$$

[当乘子是写在右边时，第二式应为 $a(\eta\Theta)=(a\eta)\Theta$]．由第一式可知 $(\eta-\Theta)a=\eta a-\Theta a$ 以及 $0\cdot a=0$（第一个零是环中的零元素，第二个零是模中的零元素）．如果乘子环是 $\mathfrak{o}$，我們就說这个模是一个 $\mathfrak{o}$-模或环 $\mathfrak{o}$ 上的模．如果环 $\mathfrak{o}$ 有一个单位元 ε，我們經常假定这个单位元同时也是一个"单位算子"，即对 $\mathfrak{G}$ 中所有元素 a 有 $\varepsilon a=a$．

7．每一个模都容許普通的整数 n 作为它的算子，因为我們有

$$n(a+b)=na+nb.$$

这时所有子模都是可許的．

8．一个 Abel 羣的所有自同态（即将 Abel 羣映射成它自身或它的一个眞子集的同态映射）的全体是一个算子区．如果我們利用公式(2)来定义两个自同态的和与积（在这个公式中右端的加号表示羣元素的运算），这个算子区就成为一个环．这个环称为 Abel 羣的自同态环．

从这样一些例子可以看出，带算子的羣有着多么广泛的应用范围．更多的例子可以在"綫性代数"的一章(第 II 卷)中看到．

习題． 1．两个可許子羣的交是可許子羣．同样，两个可許正規子羣

的交是可許正規子羣.

2. 两个彼此可交换的可許子羣的积 $\mathfrak{A}\mathfrak{B}$ 是一个可許子羣. 特别对于模来說:两个可許子模的和 $(\mathfrak{A}, \mathfrak{B})$ 是一个可許子模.

§ 46. 算子同构和算子同态

設 $\mathfrak{G}$ 和 $\bar{\mathfrak{G}}$ 是具有同一算子区 Ω 的两个羣. 如果已經給定了 $\mathfrak{G}$ 到 $\bar{\mathfrak{G}}$ 的某一子集之上的一个映射,对 $\mathfrak{G}$ 中每一元素 a 有 $\bar{\mathfrak{G}}$ 中一个元素 $\bar{a}$ 与之相对应,并且与积 ab 对应的元素是积 $\bar{a}\bar{b}$,而与 θa 对应的是元素 $\theta\bar{a}$,我們就說这个映射是一个算子同态. 如果象集是整个羣 $\bar{\mathfrak{G}}$,也就是說,$\bar{\mathfrak{G}}$ 中的每个元素都和 $\mathfrak{G}$ 中的一个元素相对应,那末我們所得到的就是 $\mathfrak{G}$ 到 $\bar{\mathfrak{G}}$ 之上的一个同态映射,在一般情况下所得到的只是 $\mathfrak{G}$ 到 $\bar{\mathfrak{G}}$ 之內的同态映射. 如果相应于每一 $\bar{a}$ 恰恰只有一个 a,这个同态就是一个算子同构.

記号: $\mathfrak{G}$ 到 $\bar{\mathfrak{G}}$ 之上的算子同态以 $\mathfrak{G} \sim \bar{\mathfrak{G}}$ 来表示,算子同构以 $\mathfrak{G} \cong \bar{\mathfrak{G}}$ 来表示.

如果 $\mathfrak{N}$ 是 $\mathfrak{G}$ 的一个可許正規子羣,那末在算子 θ 的作用之下陪集 $\bar{a} = a\mathfrak{N}$ 中的元素 ab 变为 $\theta a \cdot \theta b$,卽变为陪集 $\theta a \cdot \mathfrak{N}$ 中的一个元素. 这个陪集 $\overline{\theta a}$ 称为算子 θ 和陪集 $\bar{a}$ 的积. 这样一来,商羣 $\mathfrak{G}/\mathfrak{N}$ 就成了一个具有同一算子区 Ω 的带算子羣,而 $a \to \bar{a}$ 則是一个算子同态.

反之,从一个算子同态出发,象在 § 13 中所作的那样,可以得出下面的同态定理:

如果 $\mathfrak{G} \sim \bar{\mathfrak{G}}$,則 $\mathfrak{G}$ 中被映射成 $\bar{\mathfrak{G}}$ 中的单位元素的元素的集合 $\mathfrak{N}$ 是 $\mathfrak{G}$ 中的一个可許正規子羣,而 $\mathfrak{N}$ 的陪集和 $\bar{\mathfrak{G}}$ 中的元素双方单值且算子同构地相对应,卽

$$\mathfrak{G}/\mathfrak{N} \cong \bar{\mathfrak{G}}.$$

在§13中我們已經知道了$\mathfrak{N}$是一个正規子羣。$\mathfrak{N}$为可許子羣这一点是很显然的，因为如果a被映射成$\bar{e}$，則Θa将被映射成$\Theta\bar{e}=\bar{e}$，这就是說，$\mathfrak{N}$在包含a的同时也包含着Θa。我們早就知道，陪集和$\bar{\mathfrak{G}}$的元素的对应是一个双方单值的对应。由于原先給定的对应$\mathfrak{G}\to\bar{\mathfrak{G}}$是一个算子同态，这个对应同时也是一个算子同构。

对于具有算子区$\mathfrak{o}$的加法羣($\mathfrak{o}$-模，其中一个特例就是$\mathfrak{o}$中的理想)，算子同态也称为**模同态**。我們注意，在一个模同态之下Θa变为$\Theta\bar{a}$，因此Θ是保持不变的。这就是模同态和环同态的差别所在，在一个环同态下ab变为$\bar{a}\bar{b}$。讓我們举一个例子来說明这一点。我們考慮环$\mathfrak{o}$中两个理想，并把它們看成$\mathfrak{o}$模。算子同态把每个a映射成$\bar{a}$并把ra映射成$r\bar{a}$(对$\mathfrak{o}$中任意r)。这两个理想也可以看成两个环，环同态把积ra(r在理想之內)不是映成$r\bar{a}$，而是映成$\bar{r}\bar{a}$。

在下面凡是講到"羣"的时候，我們也把带算子的羣包括在內。这时"子羣"和"正規子羣"永远理解为可許子羣和可許正規子羣，而"同构"和"同态"則理解为算子同构和算子同态。

习題． 1．在整数环中理想(1)和(2)是模同构的，但不是环同构。

2．在数偶(a_1, a_2)的环中(§14习題1)，由(1, 0)和(0, 1)所生成的理想是环同构的，但非算子同构。

§47. 两个同构定理

在同态$\mathfrak{G}\sim\bar{\mathfrak{G}}=\mathfrak{G}/\mathfrak{N}$之下$\mathfrak{G}$的每个子羣$\mathfrak{H}$都被同态地映射成$\bar{\mathfrak{G}}$的一个子羣$\bar{\mathfrak{H}}$。現在讓我們反过来从$\bar{\mathfrak{H}}$出发，去确定$\mathfrak{G}$中那样一些元素的全体$\mathfrak{K}$，它們在这个同态之下的象元(或陪集)属于$\bar{\mathfrak{H}}$。集合$\mathfrak{K}$所包含的元素可能要比$\mathfrak{H}$来得多，因为它在包含$\mathfrak{H}$中

的每个元素 a 的同时也包含着陪集 $a\mathfrak{N}$ 中的全部元素. 如命 $\mathfrak{H}\mathfrak{N}$ 表示由所有乘积 ab 所組成的羣,其中 a 属于 $\mathfrak{H}$,而 b 属于 $\mathfrak{N}$(参看 § 45 問題 2),則有 $\mathfrak{K}=\mathfrak{H}\mathfrak{N}$, 而 $\bar{\mathfrak{H}}=\mathfrak{H}\mathfrak{N}/\mathfrak{N}$. 另一方面,如果 $\mathfrak{H}$ 被同态地映成 $\bar{\mathfrak{H}}$,則 $\mathfrak{H}$ 中被映射成单位元素的元素,即 $\mathfrak{H}$ 中同时属于 $\mathfrak{N}$ 的元素,組成 $\mathfrak{H}$ 中的一个正規子羣,而 $\bar{\mathfrak{H}}$ 和 $\mathfrak{H}$ 对这个正規子羣的商羣同构. 从这里我們就得出了第一同构定理:

如果 $\mathfrak{N}$ 是 $\mathfrak{G}$ 的一个正規子羣, $\mathfrak{H}$ 是 $\mathfrak{G}$ 的一个子羣,則 $\mathfrak{H}\cap\mathfrak{N}$ 是 $\mathfrak{H}$ 的一个正規子羣,且有[1]

$$\mathfrak{H}\mathfrak{N}/\mathfrak{N}\cong\mathfrak{H}/(\mathfrak{H}\cap\mathfrak{N}).$$

被映射到 $\bar{\mathfrak{H}}$ 中去的元素的全体恰和 $\mathfrak{H}$ 相重合,当且仅当 $\mathfrak{H}$ 在包含每个元素 a 的同时也包含着整个陪集 $a\mathfrak{N}$. 也就是說,当且仅当

$$\mathfrak{H}\supseteq\mathfrak{N}.$$

因此,这样一种羣 $\mathfrak{H}\supseteq\mathfrak{N}$ 和 $\bar{\mathfrak{G}}$ 中的某些羣 $\bar{\mathfrak{H}}=\mathfrak{H}/\mathfrak{N}$ 一对一地相对应. 另一方面, $\bar{\mathfrak{G}}$ 中的每个子羣 $\bar{\mathfrak{H}}$ 决定 $\mathfrak{G}$ 中一个子羣 $\mathfrak{H}\supseteq\mathfrak{N}$, 这个子羣由所有出現在 $\bar{\mathfrak{H}}$ 中的 $\mathfrak{N}$ 的陪集的所有元素組成. 最后, $\bar{\mathfrak{H}}$ 在 $\bar{\mathfrak{G}}$ 中的左、右陪集分别和 $\mathfrak{H}$ 在 $\mathfrak{G}$ 中的左、右陪集相对应. 如果 $\bar{\mathfrak{H}}$ 是 $\bar{\mathfrak{G}}$ 中的正規子羣,則 $\mathfrak{H}$ 是 $\mathfrak{G}$ 中的正規子羣,反之亦然. 这一結論在証明下面的第二同构定理的过程中还可通过另一途径得到:

如果 $\bar{\mathfrak{G}}=\mathfrak{G}/\mathfrak{N}$, 而 $\bar{\mathfrak{H}}$ 是 $\bar{\mathfrak{G}}$ 中的正規子羣,則相应的子羣 $\mathfrak{H}$ 是 $\mathfrak{G}$ 的正規子羣,且有

$$\mathfrak{G}/\mathfrak{H}\cong\bar{\mathfrak{G}}/\bar{\mathfrak{H}}. \tag{1}$$

証明. 我們有 $\mathfrak{G}\sim\bar{\mathfrak{G}}$ 和 $\bar{\mathfrak{G}}\sim\bar{\mathfrak{G}}/\bar{\mathfrak{H}}$, 从而 $\mathfrak{G}\sim\bar{\mathfrak{G}}/\bar{\mathfrak{H}}$. 因此,

---

1) 在模的情形我們自然可把 $\mathfrak{H}\mathfrak{N}$ 写成 $(\mathfrak{H},\mathfrak{N})$.

$\mathfrak{G}/\mathfrak{H}$ 和羣 $\mathfrak{G}$ 对它的一个正規子羣的商羣同构。 这个正規子羣是由 $\mathfrak{G}$ 中那样一些元素組成的，它們被同态 $\mathfrak{G}\sim\mathfrak{G}/\mathfrak{H}$ 映射成单位元素，即被第一个同态 $\mathfrak{G}\sim\bar{\mathfrak{G}}$ 映射成 $\bar{\mathfrak{H}}$ 中的元素。这个正規子羣就是 $\mathfrak{H}$。証毕。

同构 (1) 也可以写成

$$\mathfrak{G}/\mathfrak{H}\cong(\mathfrak{G}/\mathfrak{N})/(\mathfrak{H}/\mathfrak{N}).$$

习題. 1. 利用第一同构定理証明：对称羣 $\mathfrak{S}_4$ 对四元羣 $\mathfrak{V}_4$(§ 12 习題 4) 的商羣和对称羣 $\mathfrak{S}_3$ 同构。

2. 用同样的方法証明：如果某个置换羣不是完全由偶置换組成的，那末它里面的偶置换組成一个指数为 2 的正規子羣。

3. 用同样的方法証明：平面的歐几里德运动羣对由平移所組成的正規子羣的商羣和平面繞一固定点的旋轉羣同构。

§ 48. 正規羣列与合成羣列

如果羣 $\mathfrak{G}$ 除了它本身和单位羣之外沒有其它的正規子羣，它就称为一个**单羣**。

例. 阶为素数的有限羣是单羣。 事实上，子羣的阶必是整个羣的阶的一个因子，因此，除了这个羣本身和单位羣之外不可能有其它子羣，当然更不可能有其他的正規子羣。 下面 (§ 50) 将要証明，当 $n>4$ 时交錯羣 $\mathfrak{A}_n$ 也是单羣。以一个域为算子区的单項模也是单的。

由羣 $\mathfrak{G}$ 的子羣构成的一个有限序列

$$\{\mathfrak{G}=\mathfrak{G}_0\supseteq\mathfrak{G}_1\supseteq\cdots\supseteq\mathfrak{G}_l=\mathfrak{E}\} \tag{1}$$

称为一个**正規羣列**，如果对于 $\nu=1,2,\cdots,l$，每个 $\mathfrak{G}_\nu$ 是 $\mathfrak{G}_{\nu-1}$ 中的正規子羣。 数 l 称为正規羣列的**长度**，商羣 $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ 称为正規羣列的**因子**。 注意：正規羣列的长度并不是羣列 (1) 中的項的个数，而是因子 $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ 的个数。

如果正規羣列 (1) 中的每个 $\mathfrak{G}_i$ 都出現在另一正規羣列

(2) $$\{\mathfrak{G} = \mathfrak{H}_1 \supseteq \cdots \supseteq \mathfrak{H}_m = \mathfrak{E}\}$$

中，我們就說 (2) 是 (1) 的一个**加細**．例如在羣 $\mathfrak{S}_4$ (§ 9) 中，正規羣列

$$\{\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset \mathfrak{B}_4 \supset \mathfrak{E}\}$$

就是正規羣列

$$\{\mathfrak{S}_4 \supset \mathfrak{B} \supset \mathfrak{E}\}$$

的一个加細(参看 § 12，习題 4)．

在一个正規羣列中，一个項可以重复出現任意多次．如果不出現这样的情况，我們就說它是一个**无重复**的正規羣列．如果一个无重复的正規羣列不能进一步加細为一个无重复的正規羣列，我們就称它为一个**合成羣列**．例如对称羣 $\mathfrak{S}_3$ 中，正規羣列

$$\{\mathfrak{S}_3 \supset \mathfrak{A}_3 \supset \mathfrak{E}\}$$

就是一个合成羣列．同样，在 $\mathfrak{S}_4$ 中羣列

$$\{\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset \mathfrak{B}_4 \supset \{1, (12)(34)\} \supset \mathfrak{E}\}$$

也是一个合成羣列．事实上，这两个羣列中每个羣在位于它前面的羣中的指数都是素数，由此即可知这两个羣列都是不可能进一步加細的．但是也存在着那样一种羣，在它們里面每个正規羣列都可以加細，这样的羣就沒有合成羣列．无限循环羣就是这样一个例子．事实上，假設在一个无限循环羣中給出了一个无重复的正規羣列

$$\{\mathfrak{G} \supset \mathfrak{G}_1 \supset \cdots \supset \mathfrak{G}_{l-1} \supset \mathfrak{E}\},$$

并設 $\mathfrak{G}_{l-1}$ 的指数为 m，那末 $\mathfrak{G}_{l-1} = \{a^m\}$，因此在 $\mathfrak{G}_{l-1}$ 和 $\mathfrak{E}$ 之間永远还可以找出一个指数为 $2m$ 的子羣 $\{a^{2m}\}$ 来．

一个正規羣列为一合成羣列，当且仅当它的任意两个相邻的項 $\mathfrak{G}_{\nu-1}$ 和 $\mathfrak{G}_\nu$ 之間除了这两个羣本身之外不再能插进 $\mathfrak{G}_{\nu-1}$ 的正

規子羣. 根据 § 47，这一条件也就是相当于說，$\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ 是单羣. 单因子 $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ 称为**合成因子**. 在上面給出的两个合成羣列的例子中，所有合成因子都是循环羣，其阶数分別为 2，3 和 2，3，2，2.

如果一个正規羣列中，所有的因子 $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ 按照某种次序分別同构于另一正規羣列的因子，我們就說，这两个正規序列是**同构的**. 例如在一个 6 阶循环羣中，正規羣列

$$\{\{a\}, \{a^2\}, \mathfrak{E}\},$$

$$\{\{a\}, \{a^3\}, \mathfrak{E}\}$$

同构，因为第一个羣列的因子是阶为 2，3 的循环羣，而第二个羣列的因子是为 3，2 的循环羣. 为了方便起見，在下面我們也用記号 $\cong$ 来表示正規羣列之間的同构关系.

如果一个正規羣列

$$\{\mathfrak{G} \supseteq \mathfrak{G}_1 \supseteq \cdots\}$$

中最末一項是 $\mathfrak{G}$ 的一个正規子羣 $\mathfrak{A}$，但这个正規子羣不一定等于 $\mathfrak{G}$，我們就說这个列是从 $\mathfrak{G}$ **到** $\mathfrak{A}$ 的一个正規羣列. 由这样一个羣列可得出商羣 $\mathfrak{G}/\mathfrak{A}$ 的一个正規羣列

$$\{\mathfrak{G}/\mathfrak{A}_1 \supseteq \mathfrak{G}_1/\mathfrak{A} \supseteq \cdots \mathfrak{A}/\mathfrak{A} = \mathfrak{E}\},$$

反之亦然. 根据第二同构定理，第二个羣列的因子和第一个羣列的因子同构.

如果两个正規羣列

$$\{\mathfrak{G} \supseteq \mathfrak{G}_1 \supseteq \cdots \supseteq \mathfrak{G}_r = \mathfrak{E}\}$$

和

$$\{\mathfrak{G} \supseteq \mathfrak{H}_1 \supseteq \cdots \supseteq \mathfrak{H}_r = \mathfrak{E}\}$$

同构，那末任給第一个羣列的一个加細可以作出第二个羣列的一个加細和它同构. 事实上，每个因子 $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ 都和一个完全确定的

因子 $\mathfrak{H}_{\mu-1}/\mathfrak{H}_\mu$ 同构. 任給 $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ 的一个正規羣列可以相应地得出 $\mathfrak{H}_{\mu-1}/\mathfrak{H}_\mu$ 的一个同构的正規羣列. 因此,任給一个从 $\mathfrak{G}_{\nu-1}$ 到 $\mathfrak{G}_\nu$ 的正規羣列,可以相应地得出一个从 $\mathfrak{H}_{\mu-1}$ 到 $\mathfrak{H}_\mu$ 的同构的正規羣列来.

現在我們可以証明下面的正規羣列基本定理了,这个定理是由 O. Schreier 所首先証明的:任意羣 $\mathfrak{G}$ 的任意两个正規羣列

$$\{\mathfrak{G} \supsetneqq \mathfrak{G}_1 \supsetneqq \mathfrak{G}_2 \supsetneqq \cdots \mathfrak{G}_r = \mathfrak{E}\},$$

$$\{\mathfrak{G} \supsetneqq \mathfrak{H}_1 \supsetneqq \mathfrak{H}_2 \supsetneqq \cdots \supsetneqq \mathfrak{H}_s = \mathfrak{E}\}$$

有彼此同构的加細羣列:

$$\{\mathfrak{G} \supsetneqq \cdots \supsetneqq \mathfrak{G}_1 \supsetneqq \cdots \supsetneqq \mathfrak{G}_2 \supsetneqq \cdots \mathfrak{E}\}$$

$$\cong \{\mathfrak{G} \supsetneqq \cdots \supsetneqq \mathfrak{H}_1 \supsetneqq \cdots \supsetneqq \mathfrak{H}_2 \supsetneqq \cdots \supsetneqq \mathfrak{E}\}.$$

証明. 如果 $r = 1$ 或 $s = 1$, 証明是显然的,因为这时一个羣列是 $\{\mathfrak{G} \supsetneqq \mathfrak{E}\}$, 另一羣列自然是它的一个加細.

我們先对 r 用完全归納法証明这个定理当 $s = 2$ 时成立, 然后再对 s 用完全归納法証明它对任意 s 成立.

当 $s = 2$ 时,第二个羣列是这种形式:

$$\{\mathfrak{G} \supsetneqq \mathfrak{H} \supsetneqq \mathfrak{E}\}.$$

我們命 $\mathfrak{D} = \mathfrak{G}_1 \cap \mathfrak{H}$, $\mathfrak{P} = \mathfrak{G}_1\mathfrak{H}$. 这时 $\mathfrak{D}$ 和 $\mathfrak{P}$ 都是 $\mathfrak{G}$ 中的正規子羣. 当然有可能出現 $\mathfrak{P} = \mathfrak{G}$ 或 $\mathfrak{D} = \mathfrak{E}$ 的情况. 根据归納假設,长度分别为 $r - 1$ 和 2 的正規羣列

$$\{\mathfrak{G}_1 \supsetneqq \mathfrak{G}_2 \supsetneqq \cdots \supsetneqq \mathfrak{G}_r = \mathfrak{E}\} \quad 与 \quad \{\mathfrak{G}_1 \supseteqq \mathfrak{D} \supsetneqq \mathfrak{E}\}$$

有彼此同构的加細羣列

$$(3) \qquad \begin{cases} \{\mathfrak{G}_1 \supsetneqq \cdots \supsetneqq \mathfrak{G}_2 \supsetneqq \cdots \supsetneqq \mathfrak{E}\} \\ \qquad \cong \{\mathfrak{G}_1 \supsetneqq \cdots \supsetneqq \mathfrak{D} \supsetneqq \cdots \supsetneqq \mathfrak{E}\}. \end{cases}$$

其次,根据第一同构定理有

$$\mathfrak{P}/\mathfrak{H} \cong \mathfrak{G}_1/\mathfrak{D}, \quad \mathfrak{P}/\mathfrak{G}_1 \cong \mathfrak{H}/\mathfrak{D},$$

因此

(4) $$\{\mathfrak{P} \supseteq \mathfrak{G}_1 \supseteq \mathfrak{D} \supseteq \mathfrak{E}\} \cong \{\mathfrak{P} \supseteq \mathfrak{H} \supseteq \mathfrak{D} \supseteq \mathfrak{E}\}.$$

(3) 的右端乃是(4)的左端的一个加細. 相应于这个加細,我們可以找到 (4) 的右端的一个与之同构的加細:

(5) $$\{\mathfrak{P} \supseteq \mathfrak{G}_1 \supseteq \cdots \supseteq \mathfrak{D} \supseteq \cdots \supseteq \mathfrak{E}\} \cong \{\mathfrak{P} \supseteq \cdots \supseteq \mathfrak{H} \supseteq \cdots \supseteq \mathfrak{D} \supseteq \cdots \supseteq \mathfrak{E}\}.$$

由 (3) 和 (5) 卽得

$$\{\mathfrak{G} \supseteq \mathfrak{P} \supseteq \mathfrak{G}_1 \supseteq \cdots \supseteq \mathfrak{G}_2 \supseteq \cdots \supseteq \mathfrak{E}\} \cong \{\mathfrak{G} \supseteq \mathfrak{P} \supseteq \cdots \supseteq \mathfrak{H} \supseteq \cdots \supseteq \mathfrak{D} \supseteq \cdots \supseteq \mathfrak{E}\},$$

这样我們就对 $s = 2$ 的情形証明了基本定理.

对于任意的 s, 根据以上所証, 我們可以把第一个羣列 $\{\mathfrak{G} \supseteq \mathfrak{G}_1 \supseteq \cdots\}$ 加細,使之同构于 $\{\mathfrak{G} \supseteq \mathfrak{H}_1 \supseteq \mathfrak{E}\}$ 的一个加細:

(6) $$\{\mathfrak{G} \supseteq \cdots \supseteq \mathfrak{G}_1 \supseteq \cdots \supseteq \mathfrak{G}_2 \supseteq \cdots \supseteq \mathfrak{E}\} \cong \{\mathfrak{G} \supseteq \cdots \supseteq \mathfrak{H}_1 \supseteq \cdots \supseteq \mathfrak{E}\}.$$

根据归納假設, 右端那个羣列中出現的一个截段 $\{\mathfrak{H}_1 \supseteq \cdots \supseteq \mathfrak{E}\}$ 和羣列 $\{\mathfrak{H}_1 \supseteq \mathfrak{H}_2 \supseteq \cdots \supseteq \mathfrak{H}_s = \mathfrak{E}\}$ 有彼此同构的加細:

(7) $$\{\mathfrak{H}_1 \supseteq \cdots \supseteq \mathfrak{E}\} \cong \{\mathfrak{H}_1 \supseteq \cdots \supseteq \mathfrak{H}_2 \supseteq \cdots \supseteq \mathfrak{E}\}.$$

(7) 的左端給出 (6) 的右端的一个加細; 对于这个加細,我們可找出 (6) 的左端的一个与之同构的加細来. 这样一来,我們就有

$$\{\mathfrak{G} \supseteq \cdots \supseteq \mathfrak{G}_1 \supseteq \cdots \supseteq \mathfrak{G}_2 \supseteq \cdots \supseteq \mathfrak{E}\}$$
$$\cong \{\mathfrak{G} \supseteq \cdots \supseteq \mathfrak{H}_1 \supseteq \cdots \supseteq \mathfrak{E}\}$$
$$\cong \{\mathfrak{G} \supseteq \cdots \supseteq \mathfrak{H}_1 \supseteq \cdots \supseteq \mathfrak{H}_2 \supseteq \cdots \supseteq \mathfrak{E}\}. \text{[根据(7)]}$$

这就完成了定理的証明[1].

从两个同构的正規羣列中去掉重复出現的项, 所得的羣列仍

---

1) 另一証明由 H. Zassenhaus 給出: *Abh. Math. Sem. Hamburg*, **10** (1934), 106.

是同构的. 因此我們可以将基本定理中所講到的那种加細永远理解为无重复的加細.

对具有合成羣列的羣来說，由正規羣列的基本定理立卽可以得出以下两个定理.

1. **Jordan-Hölder 定理.** 同一羣 $\mathfrak{G}$ 的任意两个合成羣列彼此同构.

事实上，这两个羣列和它們的无重复加細相同.

2. 如果 $\mathfrak{G}$ 有一个合成羣列，那末 $\mathfrak{G}$ 的任何一个正規羣列都可以加細成为一个合成羣列；特别，任給 $\mathfrak{G}$ 的一个正規子羣都可找出 $\mathfrak{G}$ 的一个合成羣列来，使之以这个正規子羣为它的一个項.

如果一个羣具有一个正規羣列，它的每个因子都是 Abel 羣，这个羣就称为可解的.（例：羣 $\mathfrak{S}_3$ 和 $\mathfrak{S}_4$ 都是可解羣.）

由基本定理可知，在一个可解羣中任何一个正規羣列都可以加細成为一个具有 Abel 因子的正規羣列. 特别，如果这个羣具有合成羣列，那末每个合成因子都是单 Abel 羣；在普通的有限羣的情形，这些因子就是阶为素数的循环羣（参看下面的习題 3）.

习題. 1. 每个有限羣都有合成羣列.

2. 試作出阶为 20 的循环羣的所有的合成羣列.

3. 一个（不带算子的）Abel 羣是单羣，当且仅当它是一个素数阶循环羣.

4. 一个阶为 p^n 的羣是单羣，当且仅当 $n=1$ [参看 §12 习題 9].

5. 每个阶为 p^n 的羣都是可解的[作出这个羣的一个合成羣列，并利用习題 4].

§49. 直　　积

羣 $\mathfrak{G}$ 称为它的子羣 $\mathfrak{A}$ 和 $\mathfrak{B}$ 的直积，如果下面的条件能被滿足：

A1. $\mathfrak{A}$ 和 $\mathfrak{B}$ 是 $\mathfrak{G}$ 中的正規子羣；

A2. $\mathfrak{G} = \mathfrak{A}\mathfrak{B}$;

A3. $\mathfrak{A} \cap \mathfrak{B} = \mathfrak{E}$.

与此等价的条件是：

B1. $\mathfrak{G}$ 中每个元素可表成积

$$g = ab \quad a \in \mathfrak{A}, \quad b \in \mathfrak{B} \tag{1}$$

的形式；

B2. 因子 a 和 b 由 g 唯一确定；

B3. $\mathfrak{A}$ 的每个元和 $\mathfrak{B}$ 的每个元可交換.

由 A 可以推出 B. 事实上，B1 可由 A2 得出. B2 可由下面的考虑得出：如果 $g = a_1b_1 = a_2b_2$，則 $a_2^{-1}a_1 = b_2b_1^{-1}$. 这就是説，元素 $a_2^{-1}a_1$ 既属于 $\mathfrak{A}$ 也属于 $\mathfrak{B}$. 因此，根据 A3 这个元素必等于单位元，由此卽有

$$a_1 = a_2, \quad b_1 = b_2,$$

这样就得出了表示方式的唯一性. B3 可由下面的事实得出：由于条件 A1，积 $aba^{-1}b^{-1}$ 既属于 $\mathfrak{A}$ 也属于 $\mathfrak{B}$. 因此，根据 A3 它应等于单位元素.

由 B 可以推出 A. $\mathfrak{A}$ 为正規子羣这一点可以这样来証明：

$$g\mathfrak{A}g^{-1} = ab\mathfrak{A}b^{-1}a^{-1} = a\mathfrak{A}a^{-1} = \mathfrak{A} \qquad [\text{由于 B3}].$$

A2 可由 B1 得出. A3 可以証明如下：如果 c 是 $\mathfrak{A} \cap \mathfrak{B}$ 中的一个元素，则 c 能用两种方法表成 $\mathfrak{A}$ 中一个元素和 $\mathfrak{B}$ 中一个元素的积：

$$c = c \cdot 1 = 1 \cdot c.$$

由于表示的唯一性 [B2]，必有 $c = 1$. 这就証明了 A3.

如果 $\mathfrak{A}\mathfrak{B}$ 是一个直积，我們就把它記成 $\mathfrak{A} \times \mathfrak{B}$. 在加羣(模)的情形，我們用 $(\mathfrak{A}, \mathfrak{B})$ 来表示和，而用 $\mathfrak{A} + \mathfrak{B}$ 来表示直和.

如果 $\mathfrak{A}$ 和 $\mathfrak{B}$ 的結构已經确定，那末 $\mathfrak{G}$ 的結构也就随之确定.

事实上，任意两个元素 $g_1 = a_1b_1$ 和 $g_2 = a_2b_2$ 相乘时，只要将它們的因子相乘就行了：

$$g_1g_2 = a_1a_2 \cdot b_1b_2.$$

羣 $\mathfrak{G}$ 称为多个子羣的直积 $\mathfrak{G} = \mathfrak{A}_1 \times \mathfrak{A}_2 \times \cdots \times \mathfrak{A}_n$，如果下面的条件被满足：

A′1. 所有的 $\mathfrak{A}_\nu$ 都是 $\mathfrak{G}$ 中的正規子羣；

2. $\mathfrak{A}_1\mathfrak{A}_2\cdots\mathfrak{A}_n = \mathfrak{G}$；

3. $(\mathfrak{A}_1\mathfrak{A}_2\cdots\mathfrak{A}_{\nu-1}) \cap \mathfrak{A}_\nu = \mathfrak{E} \qquad (\nu = 2, 3, \cdots, n)$.

如果这些条件被满足，那末羣 $\mathfrak{A}_1, \mathfrak{A}_2, \cdots, \mathfrak{A}_{n-1}$ 也是它們的积 $\mathfrak{A}_1\mathfrak{A}_2\cdots\mathfrak{A}_{n-1}$ 中的正規子羣. 因此，根据同一定义，这个积也是直积. 其次，由于 $\mathfrak{A}_1\mathfrak{A}_2\cdots\mathfrak{A}_{n-1}$ 是正規子羣的积，它本身也是 $\mathfrak{G}$ 中的一个正規子羣，并且有 $(\mathfrak{A}_1\mathfrak{A}_2\cdots\mathfrak{A}_{n-1}) \cap \mathfrak{A}_n = \mathfrak{E}$，因此

(2) $$\mathfrak{G} = (\mathfrak{A}_1\mathfrak{A}_2\cdots\mathfrak{A}_{n-1}) \times \mathfrak{A}_n = \mathfrak{B}_n \times \mathfrak{A}_n,$$

其中

$$\mathfrak{B}_n = \mathfrak{A}_1\mathfrak{A}_2\cdots\mathfrak{A}_{n-1} = \mathfrak{A}_1 \times \mathfrak{A}_2 \times \cdots \times \mathfrak{A}_{n-1}.$$

利用 (2) 可以給 n 个因子的直积一个遞归的定义. 将定义 B 应用于 $\mathfrak{G} = \mathfrak{B}_n \times \mathfrak{A}_n$，并对 n 使用完全归納法，立即可以推出：

B′. $\mathfrak{G}$ 中每个元素 g 可以唯一地表成积

$$g = a_1a_2\cdots a_n \qquad (a_\nu \in \mathfrak{A}_\nu)$$

的形式，且 $\mathfrak{A}_\mu$ 中的每个元素和 $\mathfrak{A}_\nu (\mu \neq \nu)$ 中的每个元素可交换.

由 B′ 反过来可以推出 A′. 事实上，如命

$$\mathfrak{A}_1\mathfrak{A}_2\cdots\mathfrak{A}_{\nu-1}\mathfrak{A}_{\nu+1}\cdots\mathfrak{A}_n = \mathfrak{B}_\nu,$$

则由 B′ 可知，对于每个 ν 有

(3) $$\mathfrak{G} = \mathfrak{A}_\nu \times \mathfrak{B}_\nu.$$

因此每个 $\mathfrak{A}_\nu$ 都是 $\mathfrak{G}$ 中的正規子羣，并且

$$\mathfrak{A}_\nu \cap \mathfrak{B}_\nu = \mathfrak{E} \qquad (\nu = 1, 2, \cdots, n).$$

最后一个断言的内容比条件 A'3 还要多.

根据第一同构定理,由 (3) 可以推出

$$\mathfrak{G}/\mathfrak{A}_\nu \cong \mathfrak{B}_\nu; \quad \mathfrak{G}/\mathfrak{B}_\nu \cong \mathfrak{A}_\nu.$$

羣

$$(4) \qquad \begin{cases} \mathfrak{G} = \mathfrak{A}_1 \times \mathfrak{A}_2 \times \cdots \times \mathfrak{A}_n, \\ \mathfrak{G}_1 = \mathfrak{A}_1 \times \mathfrak{A}_2 \times \cdots \times \mathfrak{A}_{n-1}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \mathfrak{G}_{n-1} = \mathfrak{A}_1, \\ \mathfrak{G}_n = \mathfrak{E} \end{cases}$$

組成 $\mathfrak{G}$ 的一个正規羣列,其因子为 $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu \cong \mathfrak{A}_{n-\nu+1}$. 如果羣 $\mathfrak{A}_\nu$ 具有合成羣列,那末 $\mathfrak{G}$ 也有一个合成羣列,其长度等于每个因子的合成羣列的长度之和.

习题. 1. 如果 $\mathfrak{G} = \mathfrak{A} \times \mathfrak{B}$, $\mathfrak{G}'$ 是 $\mathfrak{G}$ 的一个子羣, 且 $\mathfrak{G}' \supseteq \mathfrak{A}$, 則 $\mathfrak{G}' = \mathfrak{A} \times \mathfrak{B}'$, 其中 $\mathfrak{B}'$ 等于 $\mathfrak{G}'$ 和 $\mathfrak{B}$ 的交.

2. 一个阶为 $n = r \cdot s$ (其中 $(r, s) = 1$) 的循环羣 $\{a\}$ 是它的 s 阶和 r 阶子羣 $\{a^r\}$ 和 $\{a^s\}$ 的直积.

3. 設 $\mathfrak{G}$ 是一个 n 阶循环羣, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, 則 $\mathfrak{G}$ 可表成 $p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_k^{\alpha_k}$ 阶循环羣的直积.

如果一个羣 $\mathfrak{G}$ 能够表成一些单羣的直积, 它就称为一个*完全可約羣*. 在这一情形下, 相当的正規羣列 (4) 已經是一个合成羣列. 根据 Jordan–Hölder 定理, 合成因子 $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu \cong \mathfrak{A}_{n-\nu+1}$ 除先后次序之差外,在同构的意义之下是唯一确定的.

定理. *在一个完全可約羣 $\mathfrak{G}$ 中每一个正規子羣都是一个直因子,也就是說,对每个正規子羣 $\mathfrak{H}$ 有一个分解 $\mathfrak{G} = \mathfrak{H} \times \mathfrak{B}$.*

証明. 由 $\mathfrak{G} = \mathfrak{A}_1 \times \mathfrak{A}_2 \times \cdots \times \mathfrak{A}_n$ 可知

$$(5) \qquad \mathfrak{G} = \mathfrak{H} \cdot \mathfrak{G} = \mathfrak{H} \cdot \mathfrak{A}_1 \cdot \mathfrak{A}_2 \cdots \mathfrak{A}_n.$$

在这个乘积中, 我們可以依次对每个因子 $\mathfrak{A}_1, \mathfrak{A}_2, \cdots, \mathfrak{A}_n$ 进

行如下的操作：或者把这个因子从乘积中去掉，或者把位于它之前的記号“·”改成直积記号“×”。事实上，因子 $\mathfrak{A}_k$ 和位于它之前的乘积 $\Pi = \mathfrak{H} \cdot \mathfrak{A}_1 \cdots \mathfrak{A}_{k-1}$ 的交是 $\mathfrak{A}_k$ 中的一个正規子羣。因此这个交或者等于 $\mathfrak{A}_k$，或者等于 $\mathfrak{E}$。在第一种情形下，$\Pi \cap \mathfrak{A}_k = \mathfrak{A}_k$，我們有 $\mathfrak{A}_k \subseteq \Pi$，故因子 $\mathfrak{A}_k$ 在乘积 $\Pi\mathfrak{A}_k$ 中是多余的。在第二种情形下积 $\Pi \cdot \mathfrak{A}_k$ 是一个直积：$\Pi \cdot \mathfrak{A}_k = \Pi \times \mathfrak{A}_k$。

根据以上所証可知，在去掉多余的因子 $\mathfrak{A}$ 之后，乘积(5)即具有直积的形式：

$$\mathfrak{G} = \mathfrak{H} \times \mathfrak{A}_{i_1} \times \mathfrak{A}_{i_2} \times \cdots \times \mathfrak{A}_{i_r},$$

这就証明了我們的命題。

§ 50. 交錯羣的单純性

在 § 48 中我們曾經說过，对称羣 $\mathfrak{S}_3$ 和 $\mathfrak{S}_4$ 是可解的。与此相反，所有其余的对称羣 $\mathfrak{S}_n (n > 4)$ 都不再是可解的。虽然每个对称羣都有一个指数为 2 的正規子羣，即交錯羣 $\mathfrak{A}_n$，可是下面的定理告訴我們，合成羣列只能是直接从 $\mathfrak{A}_n$ 到 $\mathfrak{E}$。

定理。 交錯羣 $\mathfrak{A}_n (n > 4)$ 是单羣。

我們要用到下面的

引理。 如果羣 $\mathfrak{A}_n (n > 2)$ 的正規子羣 $\mathfrak{N}$ 含有一个 3-輪換，則 $\mathfrak{N} = \mathfrak{A}_n$。

引理的証明。 設 $\mathfrak{N}$ 包含輪換(123)。这时 $\mathfrak{N}$ 一定也包含着这个元素的平方(213)以及它所有的共軛元素

$$\sigma \cdot (213)\sigma^{-1} \qquad (\sigma \in \mathfrak{A}_n).$$

取 $\sigma = (12)(3k)$，其中 $k > 3$，則有

$$\sigma(213)\sigma^{-1} = (12k),$$

因此 $\mathfrak{N}$ 包含着所有形如 $(12k)$ 的輪換。另一方面，这种輪換生成

整个羣 $\mathfrak{A}_n$（§ 10，习題 10），故必有 $\mathfrak{N} = \mathfrak{A}_n$.

定理的証明.　設 $\mathfrak{N}$ 是 $\mathfrak{A}_n$ 中一个不同于 $\mathfrak{E}$ 的正規子羣，我們要証明 $\mathfrak{N} = \mathfrak{A}_n$.

我們在 $\mathfrak{N}$ 中取一个不等于 1 的置換 τ，要求它使得尽量多的数碼不动. 我們証明，τ 只变动三个数碼，而使得所有其余数碼不动.

先假定 τ 恰恰变动四个数碼. 这时 τ 必是两个对換的积，因为要作出一个恰恰变动四个数碼的偶置換，另外的可能性是不存在的. 現在設

$$\tau = (12)(34).$$

根据假設有 $n > 4$. 因此我們可用 $\sigma = (345)$ 去作 τ 的变形而得

$$\tau_1 = \sigma\tau\sigma^{-1} = (12)(45).$$

乘积 $\tau^{-1}\tau_1$ 即 3-輪換(345)，它所变动的数碼比 τ 来得少. 这是和 τ 的选擇相违背的.

現在假定 τ 所变动的数碼多于四个. 我們再一次把 τ 写成輪換的乘积，并把最长的輪換写在最前面：即

$$\tau = (1234\cdots)\cdots;$$

如果最长的輪換是 3-輪換，則有

$$\tau = (123)(4\cdots)\cdots;$$

如果 τ 中只出現 2-輪換，則

$$\tau = (12)(34)\cdots.$$

現在我們用

$$\sigma = (234)$$

来作 τ 的变形，所得到的共軛元素

$$\tau_1 = \sigma\tau\sigma^{-1}$$

在上述三种情况下分别是

$$\tau_1 = (1342\cdots)\cdots,$$
$$\tau_1 = (134)(2\cdots)\cdots,$$
$$\tau_1 = (13)(42)(56)\cdots.$$

在所有这三种情况下 $\tau_1 \neq \tau$，从而 $\tau^{-1}\tau_1 \neq 1$. 在第一种和第三种情况下，置换 $\tau^{-1}\tau_1$ 使所有数碼 $k > 4$ 全不动，因为当 $k > 4$ 时，我們有 $\tau_1 k = \tau k$. 在第二种情况下

$$\tau = (123)(4a\cdots)\cdots,$$

除 1, 2, 3, 4 和 a 之外，置换 $\tau^{-1}\tau_1$ 使得所有其余的数碼不变. 因此，$\tau^{-1}\tau_1$ 只变动五个数碼，而 τ 本身所变动的数碼多于五个.

总之，在所有三种情况下，$\tau^{-1}\tau_1$ 所变动的数碼比 τ 本身少，而这是和 τ 的定义相违的. 因此，τ 只能变动三个数碼. 这就是說，τ 是一个 3-輪换，因而根据引理应有 $\mathfrak{N} = \mathfrak{A}_n$. 定理获証.

习題. 証明：当 $n \neq 4$ 时，交错羣 $\mathfrak{A}_n$ 是对称羣 $\mathfrak{S}_n$ 中除了它本身和 $\mathfrak{E}$ 之外唯一的正規子羣.

§51. 可迁性与本原性

集合 $\mathfrak{M}$ 的一个置换羣称为在 $\mathfrak{M}$ 上可迁，如果 $\mathfrak{M}$ 中的一个元素 a 可被这个羣中的置换变为 $\mathfrak{M}$ 中所有的元素 x.

如果这一条件成立，那末任給 $\mathfrak{M}$ 中两个元素 x 和 y，一定也能在羣中找到一个置换把 x 变为 y. 事实上，由

$$\rho a = x, \quad \sigma a = y$$

可知

$$(\sigma\rho^{-1})x = y.$$

因此，在可迁性問題上，究竟从哪一个元素 a 出发，是完全沒有差别的.

如果羣 $\mathfrak{G}$ 在 $\mathfrak{M}$ 上不是可迁的（非可迁羣），則集合 $\mathfrak{M}$ 将分解成許多可迁区，即那样一些子集，它們被羣中的置换变成其自身，

而在每个这样的集合上羣是可迁的．这些子集可以根据下面的原则来确定：$\mathfrak{M}$ 中的两个元素 a 和 b 属于同一子集，当且仅当 $\mathfrak{G}$ 中可以找到一个置換 σ，使得 $\sigma a = b$．

这一性质是：1．自反的；2．对称的；3．可传的．事实上：

1．$\sigma a = a$，如果 $\sigma = 1$；

2．由 $\sigma a = b$ 即有 $\sigma^{-1} b = a$；

3．由 $\sigma a = b$，$\tau b = c$ 即有 $(\tau\sigma)a = c$．

因此，通过这样一个原則，的确可以定义 $\mathfrak{M}$ 的一个分类．

如果羣 $\mathfrak{G}$ 在 $\mathfrak{M}$ 上可迁，而 $\mathfrak{G}_a$ 是羣 $\mathfrak{G}$ 中使 $\mathfrak{M}$ 中的元素 a 不变的置換所組成的子羣，則 $\mathfrak{G}_a$ 的每个左陪集 $\tau\mathfrak{G}_a$ 把元素 a 变为同一元素 τa．$\mathfrak{G}_a$ 的左陪集在这样的方式下和 $\mathfrak{M}$ 中的元素一对一地相对应．$\mathfrak{G}_a$ 的陪集的个数(即 $\mathfrak{G}_a$ 的指数)就等于 $\mathfrak{M}$ 中的元素的个数．羣 $\mathfrak{G}$ 中使得 τa 不变的元素所組成的羣由公式

$$\mathfrak{G}_{\tau a} = \tau\mathfrak{G}_a\tau^{-1}$$

給出．

設有集合 $\mathfrak{M}$ 的一个可迁置換羣 $\mathfrak{G}$．如果集合 $\mathfrak{M}$ 可以分解成至少两个彼此不相交的集合 $\mathfrak{M}_1$，$\mathfrak{M}_2$，$\cdots$之和，其中至少有一个集合包含着两个以上的元素，而 $\mathfrak{G}$ 中的变換把每个集合 $\mathfrak{M}_\mu$ 变成一个集合 $\mathfrak{M}_\nu$，則羣 $\mathfrak{G}$ 称为**非本原的**，而集合 $\mathfrak{M}_1$，$\mathfrak{M}_2$，$\cdots$則称为**非本原区**．如果不可能作出这样的分解

$$\mathfrak{M} = \{\mathfrak{M}_1, \mathfrak{M}_2, \cdots\},$$

則羣 $\mathfrak{G}$ 称为**本原羣**．

例． Klein 四元羣是非本原的，其非本原区为

$$\{1,2\}, \{3,4\}$$

(除此之外还有其他两种分解为非本原区的方法)．另一方面，n 个对象的全置換羣(以及交錯羣)却永远是本原的．事实上，不論

用何种方式将 $\mathfrak{M}$ 分解成子集：例如

$$\mathfrak{M} = \{\{1, 2, \cdots, k\}, \{\cdots\}, \cdots\} \qquad (1 < k < n),$$

总是可以找到一个置换把子集 $\{1, 2, \cdots, k\}$ 变为 $\{1, 2, \cdots, k-1, k+1\}$，即变为这样一个子集，它和 $\{1, 2, \cdots, k\}$ 有公共元素，但也不相等。

設 $\mathfrak{M} = \{\mathfrak{M}_1, \mathfrak{M}_2, \cdots, \mathfrak{M}_r\}$ 是具有上述性质的一个分解，因而羣 $\mathfrak{G}$ 将集合 $\mathfrak{M}_\nu$ 相互置换。 对每个 ν 在羣 $\mathfrak{G}$ 中可找到一个置换把 $\mathfrak{M}_1$ 变成 $\mathfrak{M}_\nu$。 事实上，由于 $\mathfrak{G}$ 的可迁性，只要找到一个置换将 $\mathfrak{M}_1$ 中一个任意选择的元素变为 $\mathfrak{M}_\nu$ 中的一个元素即可，这个置换一定将 $\mathfrak{M}_1$ 变为 $\mathfrak{M}_\nu$。 特别，从这里可以推出，集合 $\mathfrak{M}_1, \mathfrak{M}_2, \cdots$ 都是由同样多的元素組成的。

对于集合 $\mathfrak{M}$ 上的任意可迁置换羣，下面的定理成立：

設 $\mathfrak{g}$ 是羣 $\mathfrak{G}$ 中使得 $\mathfrak{M}$ 中一个元素 a 不变的置换所組成的子羣。 如果 $\mathfrak{G}$ 是非本原的，那末一定存在一个既不同于 $\mathfrak{g}$ 也不同于 $\mathfrak{G}$ 的子羣 $\mathfrak{h}$，使得

$$\mathfrak{g} \subset \mathfrak{h} \subset \mathfrak{G}.$$

反之，如果这样一个中間羣 $\mathfrak{h}$ 存在，則 $\mathfrak{G}$ 是非本原的。 羣 $\mathfrak{h}$ 使得一个非本原区 $\mathfrak{M}_1$ 不变，而 $\mathfrak{h}$ 的左陪集将 $\mathfrak{M}_1$ 变成另一非本原区 $\mathfrak{M}_\nu$。

証明． 先設 $\mathfrak{G}$ 是非本原的，且 $\mathfrak{M} = \{\mathfrak{M}_1, \mathfrak{M}_2, \cdots\}$ 是一个非本原区分解。 設 $\mathfrak{M}_1$ 包含元素 a。 命 $\mathfrak{h}$ 为 $\mathfrak{G}$ 中使得 $\mathfrak{M}_1$ 不变的元素所組成的子羣。 由上面所作的說明可知，$\mathfrak{h}$ 包含 $\mathfrak{G}$ 中所有那样的置换，它們把 a 变为它自身或 $\mathfrak{M}_1$ 中的另一元素。 因此，我們有 $\mathfrak{g} \subset \mathfrak{h}$，且 $\mathfrak{g} \neq \mathfrak{h}$。 另一方面，$\mathfrak{G}$ 中也有那样的置换，它把 $\mathfrak{M}_1$ 变为其它的非本原区，譬如說，变为 $\mathfrak{M}_2$。 因此 $\mathfrak{h} \neq \mathfrak{G}$。 其次，如果 τ 将 $\mathfrak{M}_1$ 变为 $\mathfrak{M}_\nu$，則整个陪集 $\tau\mathfrak{h}$ 也将 $\mathfrak{M}_1$ 变为 $\mathfrak{M}_\nu$。

現在反过来假設給出了一个既不同于 $\mathfrak{g}$ 也不同于 $\mathfrak{G}$ 的羣 $\mathfrak{h}$，

并且

$$\mathfrak{g} \subset \mathfrak{h} \subset \mathfrak{G}.$$

整个羣 $\mathfrak{G}$ 可分解成陪集 $\tau\mathfrak{h}$，而每个陪集又可分解成陪集 $\sigma\mathfrak{g}$. $\mathfrak{g}$ 的每个陪集 $\sigma\mathfrak{g}$ 将 a 变为另外一个元素 σa. 因此，如果我們把它們归并成陪集 $\tau\mathfrak{h}$，則元素 σa 将归并成至少两个彼此不相交的集合 $\mathfrak{M}_1, \mathfrak{M}_2, \cdots$，其中每个集合至少由两个元素組成. 这样，集合 $\mathfrak{M}_\nu$ 是由

(1) $$\mathfrak{M}_\nu = \tau\mathfrak{h}a$$

来定义的. 任意一个另外的置换 σ 把 $\mathfrak{M}_\nu = \tau\mathfrak{h}a$ 变为一个同样类型的集合 $\sigma\tau\mathfrak{h}a$. 这就証明了羣 $\mathfrak{G}$ 的非本原性. 如命 $\mathfrak{M}_1$ 表示当 $\tau = 1$ 时由式(1)所确定的集合，則 $\mathfrak{h}$ 使得非本原区 $\mathfrak{M}_1$ 不变（因为 $\mathfrak{h}\mathfrak{M}_1 = \mathfrak{h}\mathfrak{h}a = \mathfrak{h}a = \mathfrak{M}_1$），而陪集 $\tau\mathfrak{h}$ 将 $\mathfrak{M}_1$ 变为其余的非本原区 $\mathfrak{M}_\nu$（因为 $\tau\mathfrak{h}\mathfrak{M}_1 = \tau\mathfrak{h}\mathfrak{h}a = \tau\mathfrak{h}a$）.

习題. 1. 如果 $\mathfrak{M}$ 中的元素的个数是一个素数，則每个可迁羣都是本原的.

2. 上面定义的羣 $\mathfrak{h}$ 在 $\mathfrak{M}_1$ 上是可迁的.

3. 設集合 $\mathfrak{M}$ 可分解成三个非本原区，每个非本原区由两个元素組成；并設羣的阶为 12.

問：

a) $\mathfrak{h}$ 在 $\mathfrak{G}$ 中的指数，

b) $\mathfrak{g}$ 在 $\mathfrak{h}$ 中的指数，

c) $\mathfrak{g}$ 的阶数

为何?

4. 由有限多个对象的某些置换所組成的可迁羣，其阶数能被这些对象的个数除尽.

注. 被置换的对象的个数称为置换羣的級.

第七章 Galois 理論

Galois 理論是討論一个域 **K** 的有限可分扩张，特别是討論它的同构与自同构的。 它建立了包含在一給定的正規域中的域 **K** 的扩域与某一个有限羣的子羣之間的联系，代数方程的求解問題通过这个理論得到了解决。

关于 Galois 理論的另外一种講法，見 E. Artin 的 Galois-Theory（Galois 理論）。

在本章中出現的域都是交換的，域 **K** 称为基域。

§ 52. Galois 羣

如果給了基域 **K**，那么根据 § 43，它的每个有限可分扩域 Σ 都是由一"本原元素" ϑ 生成：$\Sigma = \mathbf{K}(\vartheta)$。根据 § 41，在一适当的扩域 Ω 中，Σ 恰有 n 个"相对"同构，即保持 **K** 的元素不变的同构，这里 n 是 Σ 对于 **K** 的次数。 作为这样一个扩域 Ω 我們可以取不可約多項式 $f(x)$ 的分裂域，这里 $f(x)$ 以 ϑ 为一个根，这个分裂域是包含 Σ 的相对于 **K** 的最小正規域，我們也称它为属于 Σ 的正規域。 $\mathbf{K}(\vartheta)$ 的相对同构可以用元素 ϑ 所变到的共軛元素 $\vartheta_1, \cdots, \vartheta_n$ 来刻划。在这些同构下，元素 $\varphi(\vartheta) = \Sigma a_\lambda \vartheta^\lambda (a_\lambda \in \mathbf{K})$ 变到 $\varphi(\vartheta_\nu) = \Sigma a_\lambda \vartheta_\nu^\lambda$，因之这个同构也可称为代換 $\vartheta \to \vartheta_\nu$。

但是应該注意，元素 ϑ 与 ϑ_ν 只是明白表示同构的工具，同构的概念却完全不依賴于 ϑ 的特殊选擇。

如果 Σ 本身是正規域，那么所有的共軛域 $\mathbf{K}(\vartheta_\nu)$ 都与 Σ 重合。

因为在这个情形，首先所有的 ϑ_ν 全包含在 $\mathbf{K}(\vartheta)$ 中. 又因为 $\mathbf{K}(\vartheta_\nu)$ 是与 $\mathbf{K}(\vartheta)$ 等价的，所以也是正规的；因之反过来 ϑ 也包含在所有的 $\mathbf{K}(\vartheta_\nu)$ 中.

反之：如果 Σ 与所有的共轭域重合，那么 Σ 是正规的.

因为在这个假定下 Σ 就等于 $f(x)$ 的分裂域 $\mathbf{K}(\vartheta_1, \cdots, \vartheta_n)$，所以是正规的.

以下我們假定 $\Sigma = \mathbf{K}(\vartheta)$ 是一个正规域. 在这个假定下，把 Σ 变成它的共轭域 $\mathbf{K}(\vartheta_\nu)$ 的同构就都是 Σ 的自同构. Σ 的这些自同构（保持 $\mathbf{K}$ 的元素不变）显然組成一个阶为 n 的羣，它称为 Σ 对于 $\mathbf{K}$ 的 Galois 羣. 这个羣在我們以后的討論中起主要的作用. 用 $\mathfrak{G}$ 代表它. 我們再一次指出：Galois 羣的阶就等于域的次数 $n = (\Sigma:\mathbf{K})$.

有时我們对于非正規的有限可分扩域 Σ' 也談 Galois 羣，所指的是所属的正規域 $\Sigma \supseteq \Sigma'$ 的 Galois 羣.

为了找出这些自同构，我們并不一定要先找出域 Σ 的一个本原元素. Σ 也可以是由多次相継的添加生成的，譬如說 $\Sigma = \mathbf{K}(\alpha_1, \cdots, \alpha_m)$，于是我們先找 $\mathbf{K}(\alpha_1)$ 的同构，它把 α_1 变成共軛的元素；然后把这些同构开拓成 $\mathbf{K}(\alpha_1, \alpha_2)$ 的同构，如此一直下去.

一个重要的情形是 $\alpha_1, \cdots, \alpha_m$ 恰好是一个无重根的方程 $f(x) = 0$ 的根. 所謂方程 $f(x) = 0$ 或者多項式 $f(x)$ 的羣就是指这个方程的分裂域的 Galois 羣. 每个相对自同构把这組根变成自身；換句話說，每个自同构引起这些根的置換. 如果知道了置換，那些自同构也就知道了；因为当 $\alpha_1, \cdots, \alpha_m$ 依次地变到 $\alpha_1', \cdots, \alpha_m'$，于是 $\mathbf{K}(\alpha_1, \cdots, \alpha_m)$ 的元素作为有理函数 $\varphi(\alpha_1, \cdots, \alpha_m)$ 就变成相应的函数 $\varphi(\alpha_1', \cdots, \alpha_m')$. 因此，一个方程的羣也可以看作它的根的一个置換羣. 在談到方程的羣时所指的总是这个置換

羣.

設Δ是一个"中間域": $\mathbf{K} \subseteq \Delta \subseteq \Sigma$. 根据§38的一条定理, Δ的每个把它变成在Σ中共軛域Δ'的(相对)同构都可以开拓成Σ的一个同构,也就是 Galois 羣的一个元素. 由此推出:

两个中間域Δ, Δ'对于$\mathbf{K}$是共軛的当且仅当 Galois 羣中有一个代换把一个变到另一个.

令$\Delta = \mathbf{K}(\alpha)$, 同样地有:

Σ中两个元素α, α'对于$\mathbf{K}$是共軛的当且仅当在Σ的 Galois 羣中有一代换把一个变成另一个.

如果方程$f(x) = 0$是不可約的,那么它的所有的根都是共軛的,反之亦然. 由此推出:

方程$f(x) = 0$的羣是可迁的当且仅当这个方程在基域中是不可約的.

元素α在Σ中不同的共軛元素的个数等于α的不可約方程的次数, 如果个数为1,即α是一綫性方程的根,那么α在$\mathbf{K}$中. 由此推出:

如果Σ的一个元素α在Σ的 Galois 羣的所有代换下都保持不变,那么α属于基域$\mathbf{K}$.

由所有这些定理我們已經看到自同构羣对于研究域的性质的意义. 为了說清楚,这些定理是对有限扩张証的,但是通过"超限归納法"它們不难推广到无限扩张. 它們对于不可分扩张也是对的, 只要把域的次数换成域的簡約次数而最后一条定理的結論换成: "那么α的一个方幂α^{p^f}属于基域$\mathbf{K}$, 这里p是特征". 但是在下一节所建立的 "Galois 理論的基本定理"只对于有限可分扩张成立.

$\mathbf{K}$上的扩域Σ称为"Abel 的", 如果它的 Galois 羣是 Abel 的;

称为“循环的”，如果羣是循环的，等等．同样，一个方程称为“Abel的，循环的，本原的”，如果它的 Galois 羣是 Abel 的，循环的或者(作为根的置换羣)是本原的．

Galois 域 $GF(p^m)$ (§ 40) 給出了 Galois 羣的一个特別簡单的例子，这里是把它包含的素域 Π 作为基域．在 § 40 中考虑过的自同构 $s(\alpha \to \alpha^p)$ 以及它的方冪 $s^2, s^3, \cdots, s^m = 1$ 都保持 Π 的元素不变，因之属于 Galois 羣；但是因为域的次数也是 m，所以它們組成整个的羣．这个羣是 m 阶的循环羣．

习題． 1．如果一个方程的根的有理函数在 Galois 羣的全部置換下保持不变，那么它属于基域，反之亦然．

2．不可約三次方程的羣有哪些可能性？

3．方程的羣全由偶置換組成当且仅当判別式的平方根包含在基域中．

4．利用习题 2 与 3 求方程

$$x^3 + 2x + 1 = 0$$

在有理数域上的羣．(首先討論可約性!)

5．用平方与立方根解方程

$$x^3 - 2 = 0,$$

$$x^4 - 5x^2 + 6 = 0,$$

从而求出它們的羣．同样地对于“分圓方程”

$$x^4 + x^2 + 1 = 0,$$

$$x^4 + 1 = 0$$

(这里全是以有理数域作为基域)，求出它們的解．

§ 53. Galois 理論的基本定理

“基本定理”是：

1. 每个中間域 Δ, $\mathbf{K} \subseteq \Delta \subseteq \Sigma$，都对应着 Galois 羣 $\mathfrak{G}$ 的一个子羣 $\mathfrak{g}$，即 Σ 的保持 Δ 的元素不变的全体自同构．2. Δ 是由 $\mathfrak{g}$ 唯一决定；Δ 就是 Σ 中被 $\mathfrak{g}$ 中代換保持不变的元素的全体．3. 对于

$\mathfrak{G}$ 的每个子羣 $\mathfrak{g}$ 都有一个域 Δ，它与 $\mathfrak{g}$ 有以上的关系. 4. $\mathfrak{g}$ 的阶就等于 Σ 对于 Δ 的次数；$\mathfrak{g}$ 在 $\mathfrak{G}$ 中的指数就等于 Δ 对于 $\mathbf{K}$ 的次数.

証明. Σ 的保持 Δ 的元素不变的自同构的全体就是 Σ 对于 Δ 的 Galois 羣，当然具有羣的性质. 这就証明了断語 1. 如果把 Σ 看作扩域，Δ 看作基域，应用 § 52 最后一条定理即得 2. 比較有些困难的是断語 3.

設 $\Sigma = \mathbf{K}(\vartheta)$，$\mathfrak{g}$ 是 $\mathfrak{G}$ 的一个子羣. 我們用 Δ 代表 Σ 中被 $\mathfrak{g}$ 中所有代换 σ 保持不变的元素的全体；因为如果 α 与 β 是被代换 σ 保持不变，那么 $\alpha+\beta$，$\alpha-\beta$，$\alpha\cdot\beta$ 以及在 $\beta\neq 0$ 时 $\alpha:\beta$ 也具有这个性質. 于是 $\mathbf{K}\subseteq\Delta\subseteq\Sigma$. Σ 对于 Δ 的 Galois 羣包含羣 $\mathfrak{g}$，因为 $\mathfrak{g}$ 的代换具有保持 Δ 的元素不变的性質. 假如 Σ 对于 Δ 的 Galois 羣比羣 $\mathfrak{g}$ 包含更多的元素，則次数 $(\Sigma:\Delta)$ 就要比 $\mathfrak{g}$ 的阶来得大. 次数 $(\Sigma:\Delta)$ 等于 ϑ 对于 Δ 的次数，因为 $\Sigma=\Delta(\vartheta)$. 如果 $\sigma_1,\cdots,\sigma_h$ 是 $\mathfrak{g}$ 的全部代换，那么 ϑ 是 h 次方程

$$(1)\qquad (x-\sigma_1\vartheta)(x-\sigma_2\vartheta)\cdots(x-\sigma_h\vartheta)=0$$

的根，它的系数是被羣 $\mathfrak{g}$ 保持不变的，因而属于 Δ. 因此 ϑ 对于 Δ 的次数不能大于 $\mathfrak{g}$ 的阶.

剩下的唯一可能性就是，$\mathfrak{g}$ 恰恰是 Σ 对于 Δ 的 Galois 羣. 这証明了 3. (順便也就得出 (1) 在 $\Delta[x]$ 中的不可約性.)

最后，如果 $\mathfrak{G}$ 的阶为 n，$\mathfrak{g}$ 的阶为 h，j 是指数，則有

$$n=(\Sigma:\mathbf{K}),\quad h=(\Sigma:\Delta),\quad n=h\cdot j,$$

$$(\Sigma:\mathbf{K})=(\Sigma:\Delta)\cdot(\Delta:\mathbf{K}),$$

即

$$(\Delta:\mathbf{K})=j.$$

这就証明了 4.

根据証明了的基本定理，子羣 $\mathfrak{g}$ 与中間域 Δ 之間的对应是 1-1

的. 現在产生一个問題：在有了 Δ 之后如何找 $\mathfrak{g}$. 或者有了 $\mathfrak{g}$ 如何找 Δ?

第一个問題是容易的. 假定我們已經找到与 ϑ 共軛的元素 $\vartheta_1, \cdots, \vartheta_n$ 并且用 ϑ 表出；于是羣 $\mathfrak{G}$ 的自同构 $\vartheta \to \vartheta_\nu$ 也就有了. 現在如果給了一个子域 $\Delta = \mathbf{K}(\beta_1, \cdots, \beta_k)$，这里 $\beta_1, \cdots, \beta_k$ 对于 ϑ 的表达式是知道的，那么 $\mathfrak{g}$ 就是由 $\mathfrak{G}$ 中所有保持 $\beta_1, \cdots, \beta_k$ 不变的代換組成；因为它們也保持 $\beta_1, \cdots, \beta_k$ 的有理函数不变.

反过来，如果給了 $\mathfrak{g}$，那么作乘积

$$(x - \sigma_1\vartheta)(x - \sigma_2\vartheta)\cdots(x - \sigma_h\vartheta).$$

按照基本定理的証明，这个多項式的系数必然属于 Δ，并且生成 Δ；因为它們生成一个域，ϑ 作为方程 (1) 的根对于这个域的次数已經是 h，因之它不可能是 Δ 的子域. Δ 的生成元簡单地就是 $\sigma_1\vartheta, \cdots, \sigma_h\vartheta$ 的初等对称函数.

另外一个方法是，設法找一个元素 $\chi(\vartheta)$，它被 $\mathfrak{g}$ 中的代換保持不变，但不被 $\mathfrak{G}$ 中其他代換保持不变. 这个元素属于域 Δ，但不属于 Δ 的任一个子域，因而生成 Δ.

由 Galois 理論的基本定理我們看到，一旦知道了 Galois 羣，$\mathbf{K}$ 与 Σ 的所有的中間域就全看清楚了，它們的个数显然是有限的；因为一个有限羣只有有限多个子羣. 由羣我們还可以知道不同的域的相互包含关系；因为有定理：

如果 Δ_1 是 Δ_2 的子域，那么属于 Δ_1 的羣包含属于 Δ_2 的羣，反之亦然.

証明. 首先設 $\Delta_1 \subseteq \Delta_2$. 于是所有保持 Δ_2 的元素不变的代換也保持 Δ_1 的元素不变.

其次，設 $\mathfrak{g}_1 \supseteq \mathfrak{g}_2$，于是所有被 $\mathfrak{g}_1$ 的代換保持不变的域元素也被 $\mathfrak{g}_2$ 的代換保持不变.

作为結束我們提出下面的問題：如果我們把基域 $\mathbf{K}$ 扩大到域 Λ 同时扩域 $\mathbf{K}(\vartheta)$ 也相应地扩大到 $\Lambda(\vartheta)$，那么 $\mathbf{K}(\vartheta)$ 对于 $\mathbf{K}$ 的 Galois 羣有什么改变？（我們自然要假定，$\Lambda(\vartheta)$ 是有意义的，即 Λ 与 ϑ 都包含在一个共同的扩域 Ω 之中。）

代换 $\vartheta\to\vartheta_\nu$ 按照扩张給出 $\Lambda(\vartheta)$ 的自同构，它也給出 $\mathbf{K}(\vartheta)$ 的同构，因为 $\mathbf{K}(\vartheta)$ 正规，所以它是 $\mathbf{K}(\vartheta)$ 的自同构．因此基域扩充之后的代换羣是原来羣的子羣．如果我們特別取 $\mathbf{K}$ 与 $\mathbf{K}(\vartheta)$ 的一个中間域为 Λ，我們看到确实可能是眞子羣．但是这个子羣也可能就是原来的羣；这时我們說，基域的这个扩张沒有簡約 $\mathbf{K}(\vartheta)$ 的羣．

习题． 1．Galois 羣 $\mathfrak{G}$ 的两个子羣的交对应于属于这两个羣的子域的和域，而和羣对应于交域[1]．

2．如果域 Σ 对于 $\mathbf{K}$ 是循环的，次数为 n，那么对于 n 的每个因子 d 恰有一个次数为 d 的中間域，并且两个这样的域一个包含另一个当且仅当一个的次数被另一个的次数整除（參考 §10 最后）．

3．利用 Galois 理論重新决定 $GF(p^n)$ 的子域（§40）．

4．設 $\mathbf{K}\subseteq\Lambda$，$\mathbf{K}(\vartheta)$ 对 $\mathbf{K}$ 正規．証明：$\mathbf{K}(\vartheta)$ 对 $\mathbf{K}$ 的羣等于 $\Lambda(\vartheta)$ 对于 Λ 的羣当且仅当 $\mathbf{K}(\vartheta)\cap\Lambda=\mathbf{K}$．

5．利用 §51 的定理証明：

由添加不可約代数多項式的一个根 α_1 得到的域 $\mathbf{K}(\alpha_1)$ 有一个子域 Δ 适合

$$\mathbf{K}\subset\Delta\subset\mathbf{K}(\alpha_1),$$

当且仅当这个方程的 Galois 羣作为根的置换羣是非本原的．特別地，Δ 可以这样决定，即域次数 $(\Delta:\mathbf{K})$ 等于非本原区域的个数．

6．按以下的修改来証明关于不可分扩张（特征 p）的基本定理．断語 2 是：Σ 中被 $\mathfrak{g}$ 的代換保持不变的元素全体是"在 Σ 中 Δ 的根域"，也就是 Σ 中 p^i 次方属于 Δ 的元素的全体．断語 3 是：对应于 $\mathfrak{G}$ 的每个子羣 $\mathfrak{g}$ 恰有一个

1）所謂两个子羣的和羣是指由这两个羣的并集合生成的羣．同样地定义和域的概念．

域 Δ，它对开 p 次方是不变的并且被 $\mathfrak{g}$ 中代换也只有 $\mathfrak{g}$ 中代换保持不变。断語 4 改为对簡約次数。

§ 54. 共軛的羣、域与域的元素

設 $\mathfrak{G}$ 是 $\mathbf{\Sigma}$ 对于 $\mathbf{K}$ 的 Galois 羣，β 是 Σ 的一个元素。屬于中間域 $\mathbf{K}(\beta)$ 的子羣 $\mathfrak{g}$ 是由保持 β 不变的代换組成。$\mathfrak{G}$ 中其余的代换把 β 变到与之共軛的元素，并且每个共軛元素都可以这样得到（§ 52）。現在我們进一步断言：

$\mathfrak{G}$ 中把 β 变到某一給定的共軛元素的代换組成 $\mathfrak{g}$ 的一个陪集 $\tau\mathfrak{g}$，并且每个陪集把 β 变到同一个共軛元素。

証明. 如果 ρ 与 τ 是把 β 变到同一个共軛元素的代换：

$$\rho(\beta) = \tau(\beta),$$

那么

$$\tau^{-1}\rho(\beta) = \tau^{-1}\tau(\beta) = \beta;$$

即 $\tau^{-1}\rho = \sigma$ 是 $\mathfrak{g}$ 的一个元素，从而 $\rho = \tau\sigma$；这就是說，ρ 与 τ 屬于同一个陪集。如果 ρ 与 τ 在同一个陪集中，即都在 $\tau\mathfrak{g}$ 中，那么 $\rho = \tau\sigma$，σ 在 $\mathfrak{g}$ 中；因之

$$\rho(\beta) = \tau\sigma(\beta) = \tau(\sigma(\beta)) = \tau(\beta).$$

由这个定理重新推出，β 的次数（= 共軛元素的个数）等于 $\mathfrak{g}$ 的指数（= 陪集的个数）。

变 β 为 $\tau\beta$ 的自同构 τ 把 $\mathbf{K}(\beta)$ 变成 $\mathbf{K}(\tau\beta)$。我們断言：域 $\mathbf{K}(\tau\beta)$ 屬于子羣 $\tau\mathfrak{g}\tau^{-1}$。

因为屬于 $\mathbf{K}(\tau\beta)$ 的子羣是由保持 $\tau\beta$ 不变的代换 σ' 組成，对于它有

$$\sigma'\tau\beta = \tau\beta$$

或者

$$\tau^{-1}\sigma'\tau\beta = \beta.$$

或者

$$\tau^{-1}\sigma'\tau = \sigma \text{ 在 } \mathfrak{g} \text{ 中}$$

或者

$$\sigma' = \tau\sigma\tau^{-1},$$

这就是説，它恰为羣 $\tau\mathfrak{g}\tau^{-1}$.

因之共軛的羣屬于共軛的域.

根据 § 52，$\mathbf{K}$ 上的域 Δ 是正規的当且仅当它与所有共軛域重合．由此立即推出：

域 Δ, $\mathbf{K} \subseteq \Delta \subseteq \Sigma$，是正規的当且仅当对应的羣 $\mathfrak{g}$ 与它的所有在 $\mathfrak{G}$ 中共軛的羣 $\tau\mathfrak{g}\tau^{-1}$ 重合，也就是，它是 $\mathfrak{G}$ 的正規子羣.

如果 Δ 是正規的，那么就产生了問題：Δ 对 $\mathbf{K}$ 的羣是什么?

$\mathfrak{G}$ 中的每个自同构把 Δ 变到自身，因之都引起所求的 Δ 对于 $\mathbf{K}$ 的羣中一个自同构．$\mathfrak{G}$ 中两个自同构的乘积对应于相应的 Δ 的自同构的乘积，因之 $\mathfrak{G}$ 同态地映射到 Δ 的羣．$\mathfrak{G}$ 中对应到 Δ 的单位代换的元素恰好就是 $\mathfrak{g}$ 的元素；根据同态定理，由此推出，所求的羣同构于商羣 $\mathfrak{G}/\mathfrak{g}$．于是：

Δ 对于 $\mathbf{K}$ 的 Galois 羣同构于商羣 $\mathfrak{G}/\mathfrak{g}$.

习题. 1．Abel 域的所有子域都是正規的，同时也是 Abel 的．循环域的所有子域都也是循环的.

2．如果 $\mathbf{K} \subseteq \Delta \subseteq \Sigma$，$\Lambda$ 是对于 $\mathbf{K}$ 的包含 Δ 的最小正規域，那么 Λ 对应的羣就是 Δ 对应的羣与它所有的共軛羣的交.

3．Γ 是有理数域，$\rho = \dfrac{-1-\sqrt{-3}}{2}$ 是三次原单位根，域 $\Gamma(\rho, \sqrt[3]{2})$ 有哪些子域? 哪些子域是共軛的，哪些是正規的?

4．对于域 $\Gamma(\sqrt{2}, \sqrt{5})$ 問与上相同的問題.

§ 55. 分 圓 域

設 Γ 是有理数域，也就是特征零的素域．恰以全部 h 次原单位根为根的方程：

(1) $$\Phi_h(x)=0$$

(参考 § 39)称为分圆方程，h 次单位根的域称为分圆域或者圆域，这个名称有以下的理由：复数

$$\zeta=e^{\frac{2\pi i}{h}}=\cos\frac{2\pi}{h}+i\sin\frac{2\pi}{h}$$

是一个 h 次原单位根；由它根据方程

$$2\cos\frac{2\pi}{h}=\zeta+\zeta^{-1}$$

就决定 $\cos\frac{2\pi}{h}$，而有了这个余弦就可以作出正 h 边形的图，也就是把圆等分成 h 个弧。

以下圆域的理論自然不依賴于我們把原单位根 ζ 看作复数还是只看作一个符号。

我們首先来証明，方程 (1) 在 Γ 中是不可約的。

設 $f(x)=0$ 是任意选定的一个原单位根 ζ 所适合的不可約方程。不妨設 $f(x)$ 是一整系数的本原多項式。下面来証 $f(x)=\Phi_h(x)$。

設 p 是一个在 h 中不出現的素数，于是 ζ^p 与 ζ 同时都是 h 次原单位根，ζ^p 适合一个不可約的整系数本原方程 $g(\zeta^p)=0$。我們現在首先来証：$f(x)=\varepsilon g(x)$，这里 $\varepsilon=\pm 1$ 是整数环中的可逆元素。

多項式 x^h-1 与 $f(x)$ 有公根 ζ，与 $g(x)$ 有公根 ζ^p，因之它可以被 $f(x)$ 与 $g(x)$ 整除。假如 $f(x)$ 与 $g(x)$ 根本不同（这就是說，它們并不是只差一个可逆因子），那么 x^h-1 必定被 $f(x)g(x)$ 整除：

(2) $$x^h-1=f(x)g(x)h(x),$$

这里 $h(x)$ 根据 § 26 还是整系数多項式。多項式 $g(x^p)$ 以 ζ 为根，

因之一定被 $f(x)$ 整除：

$$g(x^p) = f(x)k(x), \tag{3}$$

$k(x)$ 仍然是一个整系数多項式。

我們現在把 (2) 与 (3) 看作模 p 的同余式。模 p 有

$$g(x^p) \equiv \{g(x)\}^p.$$

因为如果我們把右端的乘方按以下的办法来作，即首先把 $g(x)$ 写成 x 的方幂不带系数的和（譬如 $2x^3$ 写成 $x^3 + x^3$），然后按 § 33 习題 2 的規則进行計算，$\{g(x)\}^p$ 是由各个項的 p 次方組成，那么恰好得出 $g(x^p)$。于是由 (3) 推出

$$\{g(x)\}^p \equiv f(x)k(x) \quad (\mathrm{mod}\ p). \tag{4}$$

設想把 (4) 的两边分解成不可分解的因子 (mod p)。根据系数在域 $C/(p)$ 中的多項式的唯一因子分解（§ 22），$f(x)$ 的任一个素因子 $\varphi(x)$ 一定能整除 $\{g(x)\}^p$，因而能整除 $g(x)$。因之 (2) 的右端必定模 p 被 $\varphi^2(x)$ 整除，于是左端的 x^h-1 以及它的微商 hx^{h-1} 模 p 也都被 $\varphi(x)$ 整除。由 $h \not\equiv 0(\mathrm{mod}\ p)hx^{h-1}$ 只有素因子 x，它不在 $x^h - 1$ 中出現，这样就得出一个矛盾。

因之实际上 $f(x) = \pm g(x)$，ζ^p 是 $f(x)$ 的根。

我們現在进一步指出：所有的原单位根都是 $f(x)$ 的根。設 ζ^ν 是一个原单位根并且

$$\nu = p_1 \cdots p_n,$$

这里 p_i 是相同的或者不同的素因子，但它們总是与 h 互素。

因为 ζ 适合方程 $f(x) = 0$，所以根据以上証明，ζ^{p_1} 也适合 $f(x) = 0$。对素数 p_2 重复以上的过程，于是 $\zeta^{p_1p_2}$ 也适合。一直下去我們就得到（完全归納法！）ζ^ν 适合方程 $f(x) = 0$。

因此 $\Phi_h(x)$ 的根全适合方程 $f(x) = 0$；因为 $f(x)$ 不可約并且 $\Phi_h(x)$ 沒有重因子，所以有

$$\Phi_h(x) = f(x).$$

这就証明了分圓方程的不可約性[1].

在这个事实的基础上我們不难造出分圓域 $\Gamma(\zeta)$ 的 Galois 羣.

首先,这个域的次数等于 $\Phi_h(x)$ 的次数,即 $\varphi(h)$(参看 § 39). 只要知道 ζ 被变到 $\Phi_h(x)$ 的那一个根, $\Gamma(\zeta)$ 的自同构就定了. $\Phi_h(x)$ 的根都是方幂 ζ^λ, 其中 λ 与 h 互素. 令 σ_λ 是把 ζ 变到 ζ^λ 的自同构. 于是

$$\sigma_\lambda = \sigma_\mu,$$

当且仅当

$$\zeta^\lambda = \zeta^\mu$$

或者

$$\lambda \equiv \mu(h).$$

再者

$$\sigma_\lambda\sigma_\mu(\zeta) = \sigma_\lambda(\zeta^\mu) = \{\sigma_\lambda(\zeta)\}^\mu = \zeta^{\lambda\mu};$$

即

$$\sigma_\lambda\sigma_\mu = \sigma_{\lambda\mu}.$$

因之, $\Gamma(\zeta)$ 的自同构羣是同构于模 h 的与 h 互素的同余类的羣.

特别这个羣是 Abel 的. 因而所有的子羣是正規子羣,所有的子域是正規的与 Abel 的.

例. 十二次单位根. 与 12 互素的同余类由

$$1, 5, 7, 11$$

代表. 因之这些自同构可以用 $\sigma_1, \sigma_5, \sigma_7, \sigma_{11}$ 表示, 其中 σ_λ 把 ζ 变到 ζ^λ. 乘法表是:

---

1) 其它的簡单証明可看 E. Landau 以及緊接在它后面的 I. Schur 在 *Math. Z.*, **29** (1929) 中的文章.

σ_1	σ_5	σ_7	σ_{11}
σ_5	σ_1	σ_{11}	σ_7
σ_7	σ_{11}	σ_1	σ_5
σ_{11}	σ_7	σ_5	σ_1

每个元素的阶都是 2．除去这个羣本身与单位羣外还有三个子羣

1．$\{\sigma_1, \sigma_5\}$，

2．$\{\sigma_1, \sigma_7\}$，

3．$\{\sigma_1, \sigma_{11}\}$．

对应于这三个羣的是二次域，都由平方根生成．下面我們来找这三个域：

四次单位根 i，$-i$ 也是十二次单位根，因之在这个域中．$\Gamma(i)$ 就是一个二次子域．

三次单位根同样也在这个域中．因为

$$\rho = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$$

是一个三次单位根，所以 $\Gamma(\sqrt{-3})$ 是一个二次子域．

由平方根 i 与 $\sqrt{-3}$ 相乘即得 $\sqrt{3}$．因之 $\Gamma(\sqrt{3})$ 是第三个域．

我們现在問，哪些子羣属于这三个域．

由于 $\sigma_5\zeta^3 = \zeta^{15} = \zeta^3$，即 σ_5 保持 $\zeta^3 = i$ 不变，所以 $\Gamma(i)$ 属于羣 $\{\sigma_1, \sigma_5\}$．

由于 $\sigma_7\zeta^4 = \zeta^{28} = \zeta^4$，即 σ_7 保持 $\zeta^4 = \rho$ 不变，所以 $\Gamma(\sqrt{-3})$ 属于羣 $\{\sigma_1, \sigma_3\}$．

剩下的一个域 $\Gamma(\sqrt{3})$ 一定属于羣 $\{\sigma_1, \sigma_{11}\}$．

这三个域中任意两个都生成整个的域．因之单位根 ζ 一定可

以用两个平方根来表示．事实上

$$\zeta=\zeta^{-3}\zeta^{4}=i^{-1}\rho=-i\frac{-1+\sqrt{-3}}{2}=\frac{i-\sqrt{3}}{2}.$$

习題． 1．对于 $h>2$，元素 $\zeta+\zeta^{-1}$ 总是生成一个次数为 $\frac{1}{2}\varphi(h)$ 的子域．

2．决定八次单位根域的子羣与子域，并把它用平方根表示出来．

3．决定七次单位根域的子羣与子域． 域 $\Gamma(\zeta+\zeta^{-1})$ 的定义方程是什么？

現在設所討論的单位根的次数 h 是素数 q．在这个情形分圓方程为

$$\Phi_q(x)=\frac{x^q-1}{x-1}=x^{q-1}+x^{q-2}+\cdots+x+1=0.$$

它的次数是 $n=q-1$．

設 ζ 是一 q 次原单位根．

与 q 互素的同余类的羣是循环的（§ 40），因之它是由 n 个同余类

$$1,\ g,\ g^2,\ \cdots,\ g^{n-1}$$

組成，这里 g 是一个“模 q 的本原数”，也就是同余类羣的生成元．因而 Galois 羣也是循环的并且由自同构 σ 生成，σ 是把 ζ 变到 ζ^g．原单位根可以如下表示：

$$\zeta,\ \zeta^{g},\ \zeta^{g^2},\ \cdots,\ \zeta^{g^{n-1}},\ 这里\ \zeta^{g^n}=\zeta.$$

令

$$\zeta^{g^\nu}=\zeta_\nu,$$

这里 ν 可以按模 n 計算，因为

$$\zeta^{g^{n+\nu}}=\zeta^{g^\nu}.$$

我們有

$$\sigma(\zeta_i)=\sigma(\zeta^{g^i})=\{\sigma(\zeta)\}^{g^i}=(\zeta^g)^{g^i}=\zeta^{g^{i+1}}=\zeta_{i+1}.$$

因之自同构把指标增加 1. σ 作用 ν 次即得

$$\sigma^{\nu}(\zeta_i) = \zeta_{i+\nu}.$$

$\zeta_i (i = 0, 1, \cdots, n-1)$ 組成域的基. 为此我們只要証明，它們是綫性无关的. 事实上，这些 ζ_i 除去次序外与 $\zeta, \cdots, \zeta^{q-1}$ 是一样的；假定在它們之間有一綫性关系：

$$a_1\zeta + \cdots + a_{q-1}\zeta^{q-1} = 0,$$

或者消去因子 ζ：

$$a_1 + a_2\zeta + \cdots + a_{q-1}\zeta^{q-2} = 0.$$

因为 ζ 不可能适合次数 $\leqslant q-2$ 的方程，所以由此推出：

$$a_1 = a_2 = \cdots = a_{q-1} = 0;$$

因此 ζ_i 綫性无关.

这个分圓域的子域就由循环羣的子羣决定（参看 §10 最后）：

如果

$$ef = n$$

是 n 的一个正因子分解，那么就有一个阶为 f 的子羣 $\mathfrak{g}$，它由元素

$$\sigma^e, \sigma^{2e}, \cdots, \sigma^{(f-1)e}, \sigma^{fe}$$

組成，其中 σ^{fe} 是单位元素. 每个子羣都可以这样得出.

根据基本定理，对应于每个这样的子羣 $\mathfrak{g}$ 都有一个中間域 Δ，它是由所有被 σ^e 以及 $\mathfrak{g}$ 中代换保持不变的元素組成.

$$\eta_\nu = \zeta_\nu + \zeta_{\nu+e} + \zeta_{\nu+2e} + \cdots + \zeta_{\nu+(f-1)e} \tag{5}$$

$$(\nu = 0, \cdots, e-1)$$

是一些这样的元素.

由 (5) 所定义的元素 $\eta_0, \eta_1, \cdots, \eta_{e-1}$ 被 Gauss 称为圓域的 f 項周期.

每个 η_ν 被代换 σ^e 以及它的冪保持不变，但是不被 Galois 羣中其他代换保持不变. 因之每个单个的 η_ν 都是中間域 Δ 的生成

元。譬如我們取 $\nu = 0$，就有

$$\Delta = \Gamma(\eta_0)$$

$$\eta_0 = \zeta_0 + \zeta_e + \zeta_{2e} + \cdots + \zeta_{(f-1)e}$$
$$= \zeta + \zeta^{g^e} + \zeta^{g^{2e}} + \cdots + \zeta^{g^{(f-1)e}}.$$

这样就找出了圓域 $\Gamma(\zeta)$ 的全部子域.

例. 設 $\Gamma(\zeta)$ 是 17 次单位根的域：

$$q = 17; \quad n = 16.$$

$g = 3$ 是模 17 的一个本原数，因为所有与 17 互素的同余类都是同余类 3(mod 17) 的冪. 16 个元素

$$\zeta_0 = \zeta; \quad \zeta_1 = \zeta^3; \quad \zeta_2 = \zeta^9; \quad \cdots$$

組成圓域的一組基.

有次数为 2，4 与 8 的子域. 現在我們依次地来决定它們.

8 項周期是

$$\eta_0 = \zeta + \zeta^{-8} + \zeta^{-4} + \zeta^{-2} + \zeta^{-1} + \zeta^8 + \zeta^4 + \zeta^2,$$

$$\eta_1 = \zeta^3 + \zeta^{-7} + \zeta^5 + \zeta^{-6} + \zeta^{-3} + \zeta^7 + \zeta^{-5} + \zeta^6.$$

不难算出

$$\eta_0 + \eta_1 = -1,$$

$$\eta_0\eta_1 = -4.$$

因之 η_0 与 η_1 是方程

$$y^2 + y - 4 = 0 \tag{6}$$

的根，它的解是

$$\eta = -\frac{1}{2} \pm \frac{1}{2}\sqrt{17}.$$

4 項周期是

$$\xi_0 = \zeta + \zeta^{-4} + \zeta^{-1} + \zeta^4,$$

$$\xi_1 = \zeta^3 + \zeta^5 + \zeta^{-3} + \zeta^{-5},$$

$$\xi_2 = \zeta^8 + \zeta^2 + \zeta^{-8} + \zeta^{-2},$$
$$\xi_3 = \zeta^{-7} + \zeta^{-6} + \zeta^7 + \zeta^5.$$

有

$$\xi_0 + \xi_2 = \eta_0, \quad \xi_0\xi_2 = -1,$$
$$\xi_1 + \xi_3 = \eta_1, \quad \xi_1\xi_3 = -1.$$

因之 ξ_0 与 ξ_2 适合方程

(7) $$x^2 - \eta_0 x - 1 = 0.$$

同样 ξ_1 与 ξ_3 适合方程

(8) $$x^2 - \eta_1 x - 1 = 0.$$

这些方程說明，$\Gamma(\xi_0)$ 对于 $\Gamma(\eta_0)$ 是二次的，这正如我們所希望的.

两个 2 項周期是

$$\lambda^{(1)} = \zeta + \zeta^{-1},$$
$$\lambda^{(4)} = \zeta^4 + \zeta^{-4}.$$

相加与相乘即得

$$\lambda^{(1)} + \lambda^{(4)} = \xi_0,$$
$$\lambda^{(1)}\lambda^{(4)} = \zeta^5 + \zeta^{-3} + \zeta^3 + \zeta^{-5} = \xi_1.$$

因之 $\lambda^{(1)}$ 与 $\lambda^{(4)}$ 适合方程

(9) $$\Lambda^2 - \xi_0\Lambda + \xi_1 = 0.$$

最后，ζ 本身适合方程

$$\zeta + \zeta^{-1} = \lambda^{(1)}$$

或者

$$\zeta^2 - \lambda^{(1)}\zeta + 1 = 0.$$

由此可見，17 次单位根可以通过解一系列二次方程計算出.

习題. 4. 对五次单位根的域作相同的討論.

5. 証明：$\eta_0, \cdots, \eta_{e-1}$ 組成域 Δ 的一組基.

6. 証明：二次方程 (6) 到 (9) 的解是实的并且可以用圓規与直尺作出。由此得到正十七边形的一个作图法.

迄至目前为止，我們的基域一直是有理数域．如果对于基域只假定它的特征不能整除 h，那么仍然有：每个自同构把 h 次原单位根 ζ 变到一个方冪 ζ^{λ}，其中 λ 与 h 互素：

$$\sigma_{\lambda}\zeta = \zeta^{\lambda}.$$

与以前一样有方程

$$\sigma_{\lambda}\sigma_{\mu} = \sigma_{\lambda\mu}.$$

由此推出：$\mathbf{K}(\zeta)$ **的羣同构于与** h **互素的模** h **的同余类羣的一个子羣．**

当 h 是素数时，互素的同余类的羣是阶为 $h-1$ 的循环羣，因之这个 Galois 羣也是循环的，阶为 $h-1$ 的一个因子．

§56. 循环域与純粹方程

設基域 $\mathbf{K}$ 包含 n 次单位根并且它的单位元素的 n 倍不为零（即 n 不被特征整除）．于是我們断言：“**純粹**”**方程**

$$x^n - a = 0 \qquad (a \neq 0)$$

对于 $\mathbf{K}$ **的羣是循环的．**

証明．如果 ϑ 是方程的一根，那么 $\zeta\vartheta, \zeta^2\vartheta, \cdots, \zeta^{n-1}\vartheta$（这里 ζ 是一 n 次原单位根）就是其余的根[1]．因之 ϑ 就生成了根域，并且 Galois 羣的每个代换都具有形式

$$\vartheta \to \zeta^{\nu}\vartheta.$$

代换 $\vartheta \to \zeta^{\nu}\vartheta$ 与 $\vartheta \to \zeta^{\mu}\vartheta$ 的乘积为 $\vartheta \to \zeta^{\mu+\nu}\vartheta$．因而每个代换都对应一确定的单位根 ζ^{ν} 并且代换的乘积对应单位根的乘积．于是 Galois 羣同构于 n 次单位根的羣的一个子羣．因为单位根的羣是循环的，所以它的子羣，从而 Galois 羣也是循环的．

特别当方程 $x^n - a = 0$ 不可約时，所有的根 $\zeta^{\nu}\vartheta$ 与 ϑ 共軛，

1）显然这些根全不相同，因之方程是可分的．

于是 Galois 群与整个 n 次单位根的群同构．这样，它的阶是 n．

我們現在要反过来証明，$\mathbf{K}$ 上的每个 n 次的循环域都可以用純粹方程 $x^n - a = 0$ 的根生成．

設 $\Sigma = \mathbf{K}(\vartheta)$ 是一 n 次循环域，σ 是 Galois 羣的一个生成元，$\sigma^n = 1$．我們仍然假定基域 $\mathbf{K}$ 包含 n 次单位根．

設 ζ 是一个 n 次单位根，我們作"Lagrange 預解式"：

$$(1) \qquad (\zeta, \vartheta) = \vartheta_0 + \zeta\vartheta_1 + \cdots + \zeta^{n-1}\vartheta_{n-1},$$

其中 $\vartheta_\nu = \sigma^\nu\vartheta$．

在代換 σ 下，ϑ_ν 是循环地变换：

$$\sigma\vartheta_\nu = \vartheta_{\nu+1} \quad (\vartheta_n = \vartheta_0),$$

而預解式 (ζ, ϑ) 变到：

$$(2) \qquad \begin{cases} \sigma(\zeta, \vartheta) = \vartheta_1 + \zeta\vartheta_2 + \cdots + \zeta^{n-2}\vartheta_{n-1} + \zeta^{n-1}\vartheta_0 \\ \qquad\qquad = \zeta^{-1}(\vartheta_0 + \zeta\vartheta_1 + \zeta^2\vartheta_2 + \cdots + \zeta^{n-1}\vartheta_{n-1}) \\ \qquad\qquad = \zeta^{-1}(\zeta, \vartheta). \end{cases}$$

因此，n 次方冪 $(\zeta, \vartheta)^n$ 在 σ 下是不变的，这就是說，$(\zeta, \vartheta)^n$ 属于基域 $\mathbf{K}$．

重复应用 (2) 即得

$$\sigma^\nu(\zeta, \vartheta) = \zeta^{-\nu}(\zeta, \vartheta).$$

在 Galois 羣中唯一保持預解式 (ζ, ϑ) 不变的代換是恆等代換．因之，(ζ, ϑ) 生成整个的域 $\mathbf{K}(\vartheta)$．由此推出所求的結果[1]：

如果 n 次单位根在基域中并且 n 不被特征整除，那么每个 n 次循环域都可以由添加一个 n 次根得出．

如果域 Σ 是由添加方程 $f(x) = 0$ 的根 $\xi_1, \cdots, \xi_m$ 得到，那么 σ 引起这些根的一个置換，也就是数目 $1, 2, \cdots, m$ 的一个置換，

1) 实际上，这里祇能明了，如果 $(\zeta, \vartheta) \neq 0$，那么 $(\zeta, \vartheta)^n \in \mathbf{K}$ 并且 $\Sigma = \mathbf{K}((\zeta, \vartheta))$．但是可以証明，如果 $\Sigma = \mathbf{K}(\alpha)$，那么 $(\zeta, \alpha), (\zeta, \alpha^2), \cdots, (\zeta, \alpha^{n-1})$ 中至少有一个不为零．当 $(\zeta, \alpha^i) \neq 0$ 时，取 $\vartheta = \alpha^i$ 就有 $\Sigma = \mathbf{K}((\zeta, \vartheta))$，而 $(\zeta, \vartheta)^n \in \mathbf{K}$——譯者注．

把它分解成輪換，譬如說：

$$(12\cdots j)(j+1\cdots l)\cdots.$$

Galois 羣中其余的置換都是这个写出来的置換的冪，因而把 1 变成 1，2，3，…，j．假定方程 $f(x)=0$ 是不可約的，那么根 ξ_1 可以变成所有其余的根，这就是說，輪換 $(12\cdots j)$ 已經包括了全部的根．因为这个置換的阶数为 n，所以一定有 $j=n$．这个方程的次数因而也等于 n，即等于域的次数；由此可見，添加一个根已經得出了整个的域．如果代替 1，2，…，n 我們用 0，1，…，$n-1$ 把这些根編号，我們可以选 ξ_0 就是域的生成元 $\vartheta=\vartheta_0$；在适当的編号下，可以使 $\vartheta_1=\sigma\vartheta=\sigma\xi_0=\xi_1$，$\vartheta_2=\sigma\vartheta_1=\sigma\xi_1=\xi_2$，等等．因之，在适当的編号下，$f(x)$ 的根就可以取作 (1) 中的 ϑ_ν．

如果基域 **K** 不包含 n 次单位根，那么为了能够应用以上利用 n 次根的解决方法，我們必須首先把 n 次单位根添加到 **K** 中去．在添加之后，Galois 羣仍然是循环的，因为循环羣的子羣总是循环的．

現在我还要証明一些关于素数 p 次的純粹方程不可約性的結果．

如果首先还是假定基域 **K** 包含 p 次单位根，那么根据本节开始时証明的結果，它的羣是 p 阶循环羣的一个子羣，因而是整个的羣或者是单位羣．在第一个情形，所有的根都共軛，从而方程不可約．在第二个情形，所有的根在 Galois 羣的代換下都不变；因而方程在基域 **K** 中就分解成了綫性因子．因此：多項式 x^p-a 是完全分解或者是不可約．

如果 **K** 不包含单位根，我們就不能肯定这么多．但是有定理：

x^p-a 或者是不可約的或者 a 在 **K** 中是一个 p 次冪，从而在 **K** 中有分解

$$x^p - a = x^p - \beta^p$$
$$= (x - \beta)(x^{p-1} + \beta x^{p-2} + \cdots + \beta^{p-1}).$$

証明. 假設 $x^p - a$ 可約:

$$x^p - a = \varphi(x) \cdot \psi(x).$$

$x^p - a$ 在它的分裂域中分解成:

$$x^p - a = \prod_{\nu=0}^{p-1} (x - \zeta^\nu \vartheta) \qquad (\vartheta^p = a).$$

因之,其中一个因子 $\varphi(x)$ 必然是某些 $x - \zeta^\nu\vartheta$ 的乘积, $\varphi(x)$ 的常数項 $\pm b$ 一定是 $\pm \zeta'\vartheta^\mu$ 的形式,这里 ζ' 是一个 p 次单位根:

$$b = \zeta'\vartheta^\mu,$$
$$b^p = \vartheta^{p\mu} = a^\mu.$$

由 $0 < \mu < p$ 有 $(\mu, p) = 1$, 从而对于适当的整数 ρ 与 σ 有

$$\rho\mu + \sigma p = 1,$$
$$a = a^{\rho\mu} a^{\sigma p} = b^{\rho p} a^{\sigma p};$$

由此 a 是一个 p 次冪.

在 A. Capelli 的工作: Sulla riducibilità della equazioni algebriche (关于代数方程的可約性), Rendiconti Napoli 1898 与 G. Darbi 的工作: Sulla riducibilità dell'equazioni algebriche (关于代数方程的可約性). Annali di Mat. (4), 4 (1926) 中有关于純粹方程的可約性的有趣結果.

习題. 1. 如果不假定基域 **K** 中含有 n 次单位根,那么純粹方程 $x^n - a = 0$ 的羣与模 n 的綫性代換:

$$x' \equiv cx + b$$

的一个羣同构. [对应的正規域是 $K(\vartheta, \zeta)$, 羣中每个代換 σ 是:

$$\sigma\zeta = \zeta^c,$$
$$\sigma\vartheta = \zeta^b\vartheta.]$$

§ 57. 用根式解方程

我們知道,二次、三次或者四次方程的根可以由系数通过有理

运算与开方$\sqrt{\ }, \sqrt[3]{\ }$ ，···来計算(参看§59). 我們現在間，什么样的方程也具有这个性質，即它的根可以由基域 **K** 的元素經有理运算与根号表示. 在这里我們自然可以只限于討論系数在 **K** 中的不可約方程. 这个問題也就是，由 **K** 經过逐次添加元素$\sqrt[n]{a}$(a 是屬于已經造出的域) 来造一个域，它包含所給方程一个或全部的根.

这个問題的提法在某一点上还是不确切的. 在域中根号 $\sqrt[n]{\ }$ 一般地是一个多值函数，因之 $\sqrt[n]{a}$ 究竟指哪一个根是有問題的. 例如，当我們用根式来表示六次原单位根，如果簡单地表成$\sqrt[6]{1}$或者$\sqrt[12]{1}$，那么这个解答是不够滿意的，而解 $\zeta=\frac{1}{2}\pm\frac{1}{2}\sqrt{-3}$ 就滿意多了，表达式 $\frac{1}{2}\pm\frac{1}{2}\sqrt{-3}$ 对于 $\sqrt{-3}$ 的不同的值(也就是方程 $x^2+3=0$ 的解)恰恰表示了两个六次原单位根.

在这一点上可以提出的进一步的要求是，首先，所給方程全部的根都可以用形式为

$$(1) \qquad \sqrt[n]{\cdots\sqrt[m]{\cdots}+\sqrt[r]{\cdots}+\cdots+\cdots}$$

的(或类似的)表达式来表示. 其次，这个表达式对于其中出現的根式的每一个值都表示方程的解. (当然，如果根式$\sqrt[n]{a}$在表达式(1) 中不止一次出現，那么它們的取值总是相同的.)

假設第一个要求被滿足，于是第二个要求也就被滿足，因为我們可以假定对逐次添加的根式$\sqrt[n]{a}$，方程 $x^n-a=0$ 总是不可約的. 这样，$\sqrt[n]{a}$ 的所有可能的值都是共軛的元素，它們可以經过同构互变，而这些同构在以后的添加时又可以开拓成扩域的同构(参看§38). 因之当表达式对于根式 $\sqrt[n]{a}$ 的一組值表示所給方程的一个根，那么对于每一組值也就都表示方程的根，因为每一个同构总是把 **K**$[x]$ 中所給方程的根还是变成它的根.

在以上的說明之后，現在可以来叙述用根式解方程的基本定理：

1. 只要在 $\mathbf{K}$ 中不可約方程 $f(x)=0$ 的一个根可以用表达式(1)表示，且其中根号的指数不被域 $\mathbf{K}$ 的特征整除，那么这个方程的羣就是可解的（这就是說，它的合成因子是素数阶的循环羣）。2. 反之，如果方程的羣是可解的，那么方程所有的根都可以用表达式(1)表示，并且逐次添加的根式 $\sqrt[n]{a}$ 的指数是素数，方程 $x^n-a=0$ 是不可約的，这里我們假定，域 $\mathbf{K}$ 的特征是零或者是大于在合成因子的阶中出現的最大素数[1]。

这个定理实質上是說，羣的可解性与方程用根式的可解性是相应的。在定理的第一部分，用根式的可解性的要求是尽可能弱的，但是在第二部分是尽可能强的，因之定理的結論是最强的。

証明. 1. 利用

$$\sqrt[rs]{a}=\sqrt[r]{\sqrt[s]{a}},$$

我們可以使(1)中根号的指数全是素数。

我們对于 $\mathbf{K}$ 添加 p_1 次，p_2 次等等的单位根，这里 $p_1, p_2, \cdots$ 是(1)中根号的指数。这样我們有了一系列的一个接一个的循环正規扩张，它們还可以分解成素次数的扩张。一旦有了这些单位根之后，根据 § 56，$\sqrt[p]{a}$ 的添加或者根本不是扩张，或者是一个 p 次扩张。在添加了一个 $\sqrt[p]{a}$ 之后，紧跟着就添加所有与 a 共軛的元素的 p 次根；它們或者不是扩张，或者是素数次的循环扩张，这样就使我們作出的域对于 $\mathbf{K}$ 始終是正規的。最后經过一系列的循环扩张：

$$\mathbf{K}\subset\Lambda_1\subset\Lambda_2\subset\cdots\subset\Lambda_\omega, \tag{2}$$

1) 如果在解的公式中除去所写的根式外还允許用单位根，那么最后要求的条件可減弱为：域的特征不出現在合成因子的阶中。

得到一个正規域 $\Lambda_\omega = \Omega$，它包含表达式(1)，也就是 $f(x)$ 的一个根。因为域 Ω 是正規的，所以它包含 $f(x)$ 全部的根，这就是說，它包含 $f(x)$ 的分裂域 Σ。

設 $\mathfrak{G}$ 是 Ω 对于 $\mathbf{K}$ 的 Galois 羣。对于域的叙列(2)有 $\mathfrak{G}$ 的子羣的叙列：

(3) $$\mathfrak{G} \supset \mathfrak{G}_1 \supset \mathfrak{G}_2 \supset \cdots \supset \mathfrak{G}_\omega = \mathfrak{E},$$

这里每一个羣都是它前一个的正規子羣，商羣是素数阶的循环羣。这就是說，羣 $\mathfrak{G}$ 是可解的并且(3)是一个合成羣列。

屬于域 Σ 的是 $\mathfrak{G}$ 的正規子羣 $\mathfrak{H}$，根据 § 48，有一个包含 $\mathfrak{H}$ 的合成羣列，在同构之下它有相同的合成因子，只是次序可能不同：

(4) $$\mathfrak{G} \supset \mathfrak{H}_1 \supset \mathfrak{H}_2 \supset \cdots \supset \mathfrak{H} \supset \cdots \supset \mathfrak{E},$$

Σ 对于 $\mathbf{K}$ 的 Galois 羣是羣 $\mathfrak{G}/\mathfrak{H}$；它現在有合成羣列

$$\mathfrak{G}/\mathfrak{H} \supset \mathfrak{H}_1/\mathfrak{H} \supset \mathfrak{H}_2/\mathfrak{H} \supset \cdots \supset \mathfrak{H}/\mathfrak{H} = \mathfrak{E},$$

根据第二同构定理(§ 47)，它的因子与(4)中相应的因子同构，从而也是素数阶的循环羣。这就証明了定理的第一部分。

为了第二部分我們先来証明

引理. *q 次单位根(q 素数)可以用"不可約根式"(即不可約方程 $x^p - a = 0$ 的根)表示，这里假定，$\mathbf{K}$ 的特征是零或者是大于 q.*

因为对于 $q = 2$ 这个結論是显然的(二次单位根 ± 1 根本是有理数)，所以我們可以假定对于比 q 小的素数結論已得証。根据 § 55，q 次单位根的域是循环的，次数是 $q-1$ 的因子。如果把 $q-1$ 分解成素因子：$q - 1 = p_1^{\varrho_1} \cdots p_r^{\varrho_r}$，那么就可以通过一系列 p_ν 次的循环扩张作出所要的域。我們首先添加 p_1 次，$\cdots$，p_r 次单位根，它們根据归納假定是能够用根式表示的，然后对于 p_ν 次循环扩张应用 § 56 的定理，这样逐次添加的域的生成元就都可以用

根式表示．其中出現的方程 $x^{p_\nu}-a=0$ 一定是不可約的，否則域的次数就不能等于 p_ν 了．

現在我們能够来証定理的第二部分．設 Σ 是 $f(x)$ 的分裂域，$\mathfrak{G}\supset\mathfrak{G}_1\supset\cdots\supset\mathfrak{G}_l=\mathfrak{E}$ 是 Σ 对于 $\mathbf{K}$ 的 Galois 羣的一个合成羣列．相应于这一系列羣有一系列域：

$$\mathbf{K}\subset\Lambda_1\subset\cdots\subset\Lambda_l=\Sigma,$$

其中每一个对于前一个域都是正規的且是循环的．如果 $q_1, q_2, \cdots$ 是在这个系列中出現的相对次数，那么我們添加 q_1 次，q_2 次，$\cdots$ 单位根，根据引理它們可以用不可約根式表示．于是根据 § 56 的定理，$\Lambda_1, \Lambda_2, \cdots, \Lambda_l$ 的生成元都可以用根式表示，这里出現的方程 $x^{q_\nu}-a=0$ 或者是不可約的，或者是完全分解（§ 56 最后）；在后一种情形，相应根式的添加就是多余的．这就完成了証明．

如果有一个次数 q_ν 等于域的特征 p，那么結論 2 是不对的，下面是一个例子："二次的一般方程" $x^2+ux+v=0$（u, v 是添加到特征为 2 的素域中的不定元）是不可約的与可分的，并且在添加全部单位根之后仍然不可約．添加一个奇次数的不可約純粹方程的根不可能使它分解，因为这样得到的域是奇次的．添加一个二次根也不可能使它分解，因为这时域的簡約次数未变．因之，这个方程不可能用根式解．

应用． 2, 3 或 4 个文字的对称置换羣（以及它們的子羣）是可解的；这就説明了为什么 2, 3 与 4 次方程能够有解的公式（在 § 59 中給出）．5 个以及更多文字的对称羣不再是可解的（§ 50），并且我們卽将看到，对于每个次数都有以对称羣为羣的方程；因此对于 5 次以及 5 次以上的方程沒有解的一般公式．只是某些特殊的方程（例如分圓方程）才能用根式解．

羣是可解的那种域或者方程称为亚循环的．有时羣也称为亚

循环的(也就是可解的).

§58. n 次一般方程

所謂 n 次一般方程是指方程

$$(1) \qquad z^n - u_1 z^{n-1} + u_2 z^{n-2} - + \cdots + (-1)^n u_n = 0,$$

其中系数 $u_1, \cdots, u_n$ 是添加到基域 $\mathbf{K}$ 中的不定元. 如果它的根是 $v_1, \cdots, v_n$, 那么就有

$$\begin{cases} u_1 = v_1 + \cdots + v_n, \\ u_2 = v_1 v_2 + v_1 v_3 + \cdots + v_{n-1} v_n, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ u_n = v_1 v_2 \cdots v_n. \end{cases}$$

我們把一般方程(1)与另一个方程来比較, 它的根是不定元 $x_1, \cdots, x_n$, 因而它的系数是这些不定元的初等对称函数:

$$(2) \qquad \begin{cases} z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - + \cdots + (-1)^n \sigma_n \\ \quad = (z - x_1)(z - x_2) \cdots (z - x_n) = 0, \end{cases}$$

$$\begin{cases} \sigma_1 = x_1 + \cdots + x_n, \\ \sigma_2 = x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \sigma_n = x_1 x_2 \cdots x_n. \end{cases}$$

方程(2)是可分的并且它对于域 $\mathbf{K}(\sigma_1, \cdots, \sigma_n)$ 的 Galois 羣是 x_ν 的全部置换組成的对称羣; 因为每个置換都表示域 $\mathbf{K}(x_1, \cdots, x_n)$ 的自同构且保持对称函数 $\sigma_1, \cdots, \sigma_n$, 从而域 $\mathbf{K}(\sigma_1, \cdots, \sigma_n)$ 中的元素不变. 因此 $x_1, \cdots, x_n$ 的每一个被这个羣的置换保持不变的函数都属于域 $\mathbf{K}(\sigma_1, \cdots, \sigma_n)$, 也就是, x_ν 的每一个对称函数都可以被 $\sigma_1, \cdots, \sigma_n$ 有理地表出. 这样, 利用 Galois 理論我們給出了 §29 中"对称函数基本定理"一部分的一个新的証明.

§29 中的"唯一性定理", 即, 沒有不恆等于零的多項式 f 使关

系 $f(\sigma_1, \cdots, \sigma_n)$ 成立，也不难重新証明．假設

$$f(\sigma_1, \cdots, \sigma_n) = f(\Sigma x_i, \Sigma x_i x_k, \cdots, x_1 x_2 \cdots x_n) = 0,$$

那么用元素 v_i 来代不定元 x_i，这个关系仍然成立．于是就要有

$$f(\Sigma v_i, \Sigma v_i v_k, \cdots, v_1 v_2 \cdots v_n) = 0$$

或者 $f(u_1, \cdots, u_n) = 0$；因此 f 恆等于零．

由唯一性定理推知，对应

$$f(u_1, \cdots, u_n) \to f(\sigma_1, \cdots, \sigma_n)$$

不只是一个同态，而是环 $\mathbf{K}[u_1, \cdots, u_n]$ 与 $\mathbf{K}[\sigma_1, \cdots, \sigma_n]$ 的同构．它可以开拓成商域 $\mathbf{K}(u_1, \cdots, u_n)$ 与 $\mathbf{K}(\sigma_1, \cdots, \sigma_n)$ 的同构，并且根据 § 38 还可进一步开拓成根域 $\mathbf{K}(v_1, \cdots, v_n)$ 与 $\mathbf{K}(x_1, \cdots, x_n)$ 的同构，这些 v_i 按某种次序变成 x_k；但是 x_k 是可以用置換来变的，所以不妨使 v_i 变到 x_i．这就証明了：

有一个同构

$$\mathbf{K}(v_1, \cdots, v_n) \cong \mathbf{K}(x_1, \cdots, x_n),$$

它把 v_i 变成 x_i，u_i 变成 σ_i．

利用这个同构，所有关于方程(2)的定理都可以直接搬到方程(1)上．特别地，我們有：

一般方程(1)是可分的，它对于系数域 $\mathbf{K}(u_1, \cdots, u_n)$ 的 Galois 羣是对称羣．它的分裂域的次数为 $n!$．

令

$$\mathbf{K}(u_1, \cdots, u_n) = \Delta,$$
$$\mathbf{K}(v_1, \cdots, v_n) = \Sigma$$

并以 $\mathfrak{S}_n$ 表示对称羣．它总有一个指数为 2 的子羣：交錯羣 $\mathfrak{A}_n$．对应的中間域 Λ 是 2 次的，由 v_i 的任一个被 $\mathfrak{A}_n$ 保持不变，但不被 $\mathfrak{S}_n$ 保持不变的函数生成．如果 $\mathbf{K}$ 的特征不为 2，那么差积

$$\prod_{i<k}(v_i - v_k) = \sqrt{D}$$

就是这样一个函数，它的平方是方程(1)的判别式

$$D = \prod_{i<k} (v_i - v_k)^2.$$

判别式是一对称函数，因而是 u_i 的多项式．域 Λ 就有以下形式

$$\Lambda = \Delta(\sqrt{D}).$$

对于 $n > 4$，羣 $\mathfrak{A}_n$ 是单純的（§ 50），因之

$$\mathfrak{S}_n \supset \mathfrak{A}_n \supset \mathfrak{E} \tag{3}$$

是合成羣列．由此可見，当 $n > 4$，羣 $\mathfrak{S}_n$ 是不可解的，而由 § 57 得 Abel 的著名的定理：

对于 $n > 4$，n 次一般方程不能用根式解．

对于 $n = 2$ 与 $n = 3$，(3) 中合成因子是循环的．当 $n = 2$，有 $\mathfrak{A}_n = \mathfrak{E}$；当 $n = 3$，因子的阶为 2 与 3．对于 $n = 4$，合成羣列为

$$\mathfrak{S}_n \supset \mathfrak{A}_n \supset \mathfrak{B}_4 \supset \mathfrak{Z}_2 \supset \mathfrak{E}.$$

这里 $\mathfrak{B}_4$ 是"Klein 四元羣"

$$\{1, (12)(34), (13)(24), (14)(23)\}.$$

$\mathfrak{Z}_2$ 是它的任意一个 2 阶子羣．合成因子的阶为

$$2, 3, 2, 2.$$

我們在下一节即将討論的 2，3 与 4 次方程的解的方式就依賴于以上的事实．

§ 59. 二次、三次与四次方程

按一般理論，一般二次方程

$$x^2 + px + q = 0$$

的解可以通过一个二次根式表示；这个二次根可以取（参看上一节的末尾）根 x_1，x_2 的差积：

$$x_1 - x_2 = \sqrt{D}, \quad D = p^2 - 4q.$$

再由

$$x_1 + x_2 = -p$$

即得熟知的公式

$$x_1 = \frac{-p + \sqrt{D}}{2}, \quad x_2 = \frac{-p - \sqrt{D}}{2}.$$

这里当然假定基域的特征异于 2。

一般的三次方程

$$z^3 + a_1 z^2 + a_2 z + a_3 = 0$$

首先經过代換

$$z = x - \frac{1}{3} a_1$$

可以变成

$$x^3 + px + q = 0$$

的形式[1]。（相应于前一节的一般求解的理論，我們假定基域的特征不是 2 与 3。）

按照合成羣列

$$\mathfrak{S}_3 \supset \mathfrak{A}_3 \supset \mathfrak{E},$$

我們首先添加根的差积：

$$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \sqrt{D} = \sqrt{-4p^3 - 27q^2}$$

（參看 § 29 最后，令 $a_1 = 0$，$a_2 = p$，$a_3 = -q$）。添加后即得域 $\Delta(\sqrt{D})$。方程对于这个域的羣为 $\mathfrak{A}_3$，它是 3 阶的循环羣。按 § 57 的一般理論我們首先添加三次单位根：

$$(1) \qquad \rho = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}, \quad \rho^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{-3},$$

---

1) 这样作只是为了簡化公式。由以下証明很容易得出，对于原方程

$$z^3 + a_1 z^2 + a_2 z + a_3 = 0$$

公式是什么样子。

然后考虑 Lagrange 預解式：

$$(2)\qquad \begin{cases}(1,\ x_1)=x_1+x_2+x_3=0,\\(\rho,\ x_1)=x_1+\rho x_2+\rho^2x_3,\\(\rho^2,\ x_1)=x_1+\rho^2x_2+\rho x_3.\end{cases}$$

它們每一个的三次方一定能由 $\sqrt{-3}$ 与 $\sqrt{D}$ 有理表出。直接計算給出：

$$\begin{aligned}(\rho,\ x_1)^3=x_1^3+x_2^3+x_3^3&\\&+3\rho x_1^2x_2+3\rho x_2^2x_3+3\rho x_3^2x_1\\&+3\rho^2x_1x_2^2+3\rho^2x_2x_3^2+3\rho x_3x_1^2\\&+6x_1x_2x_3,\end{aligned}$$

交換 ρ 与 ρ^2 即得 $(\rho^2,\ x_1)^3$. 用 (1) 代入并考慮

$$\begin{aligned}\sqrt{D}&=(x_1-x_2)(x_1-x_3)(x_2-x_3)\\&=x_1^2x_2+x_2^2x_3+x_3^2x_1-x_1x_2^2-x_2x_3^2-x_3x_1^2\end{aligned}$$

即得

$$(\rho,\ x_1)^3=\Sigma x_1^3-\frac{3}{2}\Sigma x_1^2x_2+6x_1x_2x_3+\frac{3}{2}\sqrt{-3}\sqrt{D}.$$

其中出現的对称函数按 § 29 可以用初等对称函数 $\sigma_1, \sigma_2, \sigma_3$ 表示，也就是用方程的系数表示. 我們有

$$\begin{aligned}\sigma_1^3&=\Sigma x_1^3+3\,\Sigma x_1^2x_2+6\,x_1x_2x_3=0,\ \text{因}\ \sigma_1=0,\\-\frac{9}{2}\sigma_1\sigma_2&=\qquad\quad-\frac{9}{2}\Sigma x_1^2x_2-\frac{27}{2}x_1x_2x_3=0,\ \text{因}\ \sigma_1=0,\\\frac{27}{2}\sigma_3&=\qquad\qquad\qquad\qquad\quad\frac{27}{2}x_1x_2x_3=-\frac{27}{2}q\\\hline&\Sigma x_1^3-\frac{3}{2}\Sigma x_1^2x_2+6x_1x_2x_3=-\frac{27}{2}q;\end{aligned}$$

因之

$$(\rho,\ x_1)^3=-\frac{27}{2}q+\frac{3}{2}\sqrt{-3}\sqrt{D},$$

同样地

$$(\rho^2, x_1)^3 = -\frac{27}{2}q - \frac{3}{2}\sqrt{-3}\sqrt{D}.$$

这两个立方无理式 (ρ, x_1) 与 (ρ^2, x_1) 并不是无关的；而是

$$\begin{aligned}(\rho, x_1)(\rho^2, x_1) &= x_1^2 + x_2^2 + x_3^2 + (\rho + \rho^2)x_1x_2 + \\ &\quad + (\rho + \rho^2)x_1x_3 + (\rho + \rho^2)x_2x_3 \\ &= x_1^2 + x_2^2 + x_3^2 - x_1x_2 - x_1x_3 - x_2x_3 \\ &= \sigma_1^2 - 3\sigma_2 = -3p.\end{aligned}$$

我們必須如此决定立方根

$$(3)\qquad (\rho, x_1) = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}},$$

$$(\rho^2, x_1) = \sqrt[3]{-\frac{27}{2} - \frac{3}{2}\sqrt{-3D}}$$

使它們的乘积有

$$(4)\qquad (\rho, x_1)\cdot(\rho^2, x_1) = -3p.$$

为了算出根 x_1, x_2, x_3，我們对方程(2)分别乘以叙列 $1, 1, 1$；$1, \rho^2, \rho$；$1, \rho, \rho^2$，相加即得：

$$(5)\qquad \begin{cases} 3\cdot x_1 = \sum\limits_{\zeta}(\zeta, x_1) = (\rho, x_1) + (\rho^2, x_1), \\ 3\cdot x_2 = \sum\limits_{\zeta}\zeta^{-1}(\zeta, x_1) = \rho^2(\rho, x_1) + \rho(\rho^2, x_1), \\ 3\cdot x_3 = \sum\limits_{\zeta}\zeta^{-2}(\zeta, x_1) = \rho(\rho, x_1) + \rho^2(\rho^2, x_1). \end{cases}$$

公式(3)，(4)，(5)就是“Cardano 的解公式”. 由它們的推导过程可知，它們不仅对“一般的”，同时也对每个特殊的三次方程成立.

实根問題. 如果系数 p, q 所在的基域是一个实的数域 $\mathbf{K}$，那么有两个可能的情形：

a) 方程有一个实的和两个共軛的复根. 于是 $(x_1-x_2)(x_1-x_3)(x_2-x_3)$ 显然是純虚数，从而 $D<0$. 数 $\pm\sqrt{-3D}$ 是实数，在(3)中作为 (ρ, x_1) 我

們可以选取一个实的立方根．根据 (4) (ρ^2, x_1) 也是实数，(5) 中第一个公式給出 $3x_1$ 是两个实的立方根之和，而 x_2 与 x_3 是共軛的复数．

b) 方程有三个实根．这时，$\sqrt{D}$ 是实的，因之，$D \geqslant 0$．在 $D = 0$ 时(两根相等)，情况与以上一样；当 $D > 0$ 时，(3) 中在立方根下面的数就是虚数，于是在 (5) 中三个(实)数被表成**虚的**立方根的和，也就是，不是实的形式．

这个情形是所謂的三次方程的"不可約情形"．我們来証明：**在这个情形，方程**

$$x^3 + px + q = 0$$

不可能用实的根式来解，除非方程在基域中已經分解．

設方程 $x^3 + px + q = 0$ 在 $\mathbf{K}$ 中不可約并有三个实根 x_1, x_2, x_3．我們首先添加 $\sqrt{D}$．这时方程不可能分解(因为在最高是二次的域 $\mathbf{K}(\sqrt{D})$ 中不可能有不可約三次方程的根)，而它的羣将是 $\mathfrak{A}_3$．假如方程能够在添加一系列实的根式之后分解，这里根式的指数当然可以認为是素数，那么在这一串添加中必有一"临界的"添加 $\sqrt[h]{a}$ (h 素数)，即在域 Δ 中添加了 $\sqrt[h]{a}$ 之后方程恰恰分解，而在 Δ 中方程还是不可約的．按 § 56，$x^h - a$ 在 Δ 中不可約或者 a 是 Δ 中一个数的 h 次方．后一个情形可以除外，否則 a 的实的 h 次根就要包含在 Δ 中，于是 $\sqrt[h]{a}$ 的添加不可能使方程分解．因之 $x^h - a$ 是不可約的，域 $\Delta(\sqrt[h]{a})$ 的次数恰为 h．根据假定，$\Delta(\sqrt[h]{a})$ 包含一个在 Δ 中不可約的方程 $x^2 + px + q = 0$ 的根；因而 h 被 3 整除，于是 $h = 3$ 且 $\Delta(\sqrt[3]{a}) = \Delta(x_1)$．分裂域 $\Delta(x_1, x_2, x_3)$ 对于 Δ 的次数同样也是 3；因之 $\Delta(\sqrt[3]{a}) = \Delta(x_1, x_2, x_3)$．旣然域 $\Delta(\sqrt[3]{a})$ 是正規的，所以它一定包含 $\sqrt[3]{a}$ 的共軛元素 $\rho\sqrt[3]{a}$ 与 $\rho^2\sqrt[3]{a}$，也就包含单位根 ρ 与 ρ^2．这样就得出了矛盾，因为域 $\Delta(\sqrt[3]{a})$ 是实的，而数 ρ 不是．

一般的四次方程

$$z^4 + a_1 z^3 + a_2 z^2 + a_3 z + a_4 = 0$$

也可以經过代换

$$z = x - \frac{1}{4} a_1$$

变成

$$x^4 + px^2 + qx + r = 0.$$

相应于合成羣列

$$\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset \mathfrak{B}_4 \supset \mathfrak{Z}_2 \supset \mathfrak{E}$$

有域的叙列

$$\Delta \subset \Delta(\sqrt{D}) \subset \Lambda_1 \subset \Lambda_2 \subset \Sigma.$$

仍然設Δ的特征$\neq 2,3$. 下面将看到,明显的算出D是不必要的. 域Λ_1可以由$\Delta(\sqrt{D})$添加一个元素得到,这个元素被$\mathfrak{B}_4$的代换保持不变,但不被$\mathfrak{A}_4$的代换保持不变;这样一个元素是

$$\Theta_1 = (x_1 + x_2)(x_3 + x_4).$$

这个元素除去上面指出的被$\mathfrak{B}_4$中代换保持不变外,下面的代换:

$$(12), (34), (1324), (1423)$$

也保持它不变(这些代换与$\mathfrak{B}_4$合在一起成一8阶的羣). 它对于Δ有三个共轭元素,它們由$\mathfrak{S}_4$中的代换互变,即

$$\Theta_1 = (x_1 + x_2)(x_3 + x_4),$$
$$\Theta_2 = (x_1 + x_3)(x_2 + x_4),$$
$$\Theta_3 = (x_1 + x_4)(x_2 + x_3).$$

这些元素是一个三次方程

$$\Theta^3 - b_1\Theta^2 + b_2\Theta - b_3 = 0 \tag{6}$$

的根,其中b_i是$\Theta_1, \Theta_2, \Theta_3$的初等对称函数:

$$b_1 = \Theta_1 + \Theta_2 + \Theta_3 = 2\Sigma x_1x_2 = 2p,$$
$$b_2 = \Sigma\Theta_1\Theta_2 \qquad = \Sigma x_1^2x_2^2 + 3\Sigma x_1^2x_2x_3 + 6x_1x_2x_3x_4,$$
$$b_3 = \Theta_1\Theta_2\Theta_3 \qquad = \Sigma x_1^3x_2^2x_3 + 2\Sigma x_1^3x_2x_3x_4 +$$
$$+ 2\Sigma x_1^2x_2^2x_3^2 + 4\Sigma x_1^2x_2^2x_3x_4.$$

b_2与b_3可以由x_i的初等对称函数$\sigma_1, \sigma_2, \sigma_3, \sigma_4$表示. 我們有(§ 29 的方法):

$$
\begin{array}{rl}
\sigma_2^2 = & \Sigma x_1^2x_2^2 + 2\Sigma x_1^2x_2x_3 + 6x_1x_2x_3x_4 = p^2, \\
\sigma_1\sigma_3 = & \qquad\qquad \Sigma x_1^2x_2x_3 + 4x_1x_2x_3x_4 = 0, \\
-4\sigma_4 = & \qquad\qquad\qquad\qquad -4x_1x_2x_3x_4 = -4r \\
\hline
b_2 = & \Sigma x_1^2x_2^2 + 3\Sigma x_1^2x_2x_3 + 6x_1x_2x_3x_4 = p^2 - 4r;
\end{array}
$$

$$
\begin{array}{rl}
\sigma_1\sigma_2\sigma_3 = & \Sigma x_1^3x_2^2x_3 + 3\Sigma x_1^3x_2x_3x_4 + 3\Sigma x_1^2x_2^2x_3^2 + 8\Sigma x_1^2x_2^2x_3x_4 = 0, \\
-\sigma_1^2\sigma_4 = & \qquad - \Sigma x_1^3x_2x_3x_4 \qquad\qquad\qquad - 2\Sigma x_1^2x_2^2x_3x_4 = 0, \\
-\sigma_3^2 = & \qquad\qquad\qquad\qquad - \Sigma x_1^2x_2^2x_3^2 - 2\Sigma x_1^2x_2^2x_3x_4 = -q^2 \\
\hline
b_3 = & \Sigma x_1^3x_2^2x_3 + 2\Sigma x_1^3x_2x_3x_4 + 2\Sigma x_1^2x_2^2x_3^2 + 4\Sigma x_1^2x_2^2x_3x_4 = -q^2.
\end{array}
$$

因之,方程(6)是

$$\Theta^3 - 2p\Theta^2 + (p^2 - 4r)\Theta + q^2 = 0, \tag{7}$$

这个方程称为 4 次方程的**立方預解式**；它的根 Θ_1, Θ_2, Θ_3 可以按“Cardano”用根式表示．每一个 Θ 都有一个八阶的羣保持它不变；保持这三个都不变的只有 $\mathfrak{V}_4$, 因而

$$\mathbf{K}(\Theta_1, \Theta_2, \Theta_3) = \Lambda_1.$$

域 Λ_2 由 Λ_1 添加一个元素得出．这个元素不被 $\mathfrak{V}_4$ 中全部置换保持不变，只被（譬如説）单位元素与置换 (12)(34) 保持不变．$x_1 + x_2$ 是一个这样的元素．我們有

$$(x_1+x_2)(x_3+x_4)=\Theta_1 \quad 与 \quad (x_1+x_2)+(x_3+x_4)=0,$$

由此得

$$x_1 + x_2 = \sqrt{-\Theta_1}; \quad x_3 + x_4 = -\sqrt{-\Theta_1}.$$

同样有

$$x_1 + x_3 = \sqrt{-\Theta_2}; \quad x_2 + x_4 = -\sqrt{-\Theta_2};$$

$$x_1 + x_4 = \sqrt{-\Theta_3}; \quad x_2 + x_3 = -\sqrt{-\Theta_3}.$$

这三个无理式并不是沒有关系的；而是

$$
\begin{aligned}
\sqrt{-\Theta_1}\cdot\sqrt{-\Theta_2}\cdot\sqrt{-\Theta_3} &= (x_1 + x_2)(x_1 + x_3)(x_1 + x_4) \\
&= x_1^3 + x_1^2(x_2 + x_3 + x_4) + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\
&= x_1^2(x_1 + x_2 + x_3 + x_4) + \Sigma x_1x_2x_3 \\
&= \Sigma x_1x_2x_3 = -q.
\end{aligned}
$$

为了由 $\mathfrak{V}_4$ 降到 $\mathfrak{E}$ 或者由 Λ 上升到 Σ，我們恰需要两个二次无理式；因为 $\mathfrak{V}_4$ 是 4 阶的并且有 2 阶的子羣．事实上，x_i 可以由三个元素 Θ（其中的两个已經够了）有理地决定；因为

$$\begin{cases} 2x_1 = \sqrt{-\Theta_1} + \sqrt{-\Theta_2} + \sqrt{-\Theta_3}, \\ 2x_2 = \sqrt{-\Theta_1} - \sqrt{-\Theta_2} - \sqrt{-\Theta_3}, \\ 2x_3 = -\sqrt{-\Theta_1} + \sqrt{-\Theta_2} - \sqrt{-\Theta_3}, \\ 2x_4 = -\sqrt{-\Theta_1} - \sqrt{-\Theta_2} + \sqrt{-\Theta_3}. \end{cases}$$

这就是一般的四次方程解的公式．由推导过程可知，它对每个特殊的 4 次方程也成立．

注意． 由

$$\Theta_1 - \Theta_2 = -(x_1 - x_4)(x_2 - x_3),$$
$$\Theta_1 - \Theta_3 = -(x_1 - x_3)(x_2 - x_4),$$
$$\Theta_2 - \Theta_3 = -(x_1 - x_2)(x_3 - x_4)$$

可見，立方預解式的判别式等于原方程的判别式．因为我們已經知道了三次方程的判别式，所以这就給出了計算 4 次方程判别式的一个簡单方法；我們不难得出：

$$D = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3.$$

习题． 1．一个給定四次方程的立方預解式的羣是原方程的羣对于它与四元羣 $\mathfrak{V}_4$ 的交的商羣．

2．决定方程

$$x^4 + x^2 + x + 1 = 0$$

的羣．［参考 § 52 习題 3 以及上面的习題 1．］

§ 60．圓规与直尺作图

我們要来討論問題：一个几何作图問題在什么时候可以用圓規与直尺解决[1]？

1) 关于这个間題的历史最好参看 A. D. Steele, Die Rolle von Zirkel und Lineal in der griechischen Mathematik（在希腊数学中圓规与直尺的作用），Quellen und Studien Gesch. Math., **3** (1936), 287.

假設已知一些初等几何的图形(点,直綫或者圓). 問題就是,满足什么样的条件,就可以由它們作出另外一些图形.

对于已知的图形,設想已引入一个直角坐标系. 所有已知的图形就可以用数(坐标)来表示,要作的图形同样也用数表示. 如果我們能作出后面这些数(作为綫段),那么問題就解决了. 全部問題就归結为由一些已知的綫段来作綫段. 設a, b, $\cdots$是已知綫段,x是要作的綫段.

現在我們首先可以給出可构造性的一个充分条件:

如果問題的解x是实的并且能够由已知綫段a, b, $\cdots$經过有理运算以及开平方根(不一定是实的)算出,那么綫段x可以用圓規与直尺作出.

为了清楚地給出定理的証明,我們把在計算x的过程中出現的复数$p+iq$按熟知的方法用一张平面上直角坐标为p, q的点来表示,而所有要作的运算都用平面上的几何作图来实現. 实現的方法就按照:加法是向量加法,减法是它的逆运算. 乘法就是幅角相加而模相乘;如果相乘的两个数的幅角是φ_1, φ_2,模是r_1, r_2,那么乘积的幅角与模φ, r即按方程

$$\varphi=\varphi_1+\varphi_2 \quad 与 \quad r=r_1r_2 \quad 或者 \quad 1:r_1=r_2:r$$

来构造. 除法又是它的逆运算. 最后,为了計算一个模为r,幅角为φ的数的平方根,由方程

$$\varphi=2\varphi_1 \quad 或者 \quad \varphi_1=\frac{1}{2}\varphi$$

与

$$r=r_1^2 \quad 或者 \quad 1:r_1=r_1:r$$

就作出要求的幅角φ_1与模r_1. 因之所有的运算全归結为圓規与直尺的熟知的作图.

这个定理的逆也成立:

如果綫段 x 可以由已知綫段 $a, b, \cdots$ 用圓規与直尺作出，那么 x 就可以由 $a, b, \cdots$ 經有理运算与平方根表示.

为了証明这个結果，我們来考察一下在作图过程中究竟要用到哪些手續. 它們有：任取一个点(在一給定的区域之內)；过两点作一直綫，作圓，最后是求两条直綫，一直綫与一圓，或者两个圓的交点.

利用我們的坐标系，这些手續全可以化为代数运算. 如果在一区域內要任取一个点，那么总可以假定它的坐标是有理数. 其余的作图，除去最后两个(圓与直綫或者圓与圓的交点)都是有理运算，而最后两个是解二次方程，也就是开平方根，这就証明了定理.

我們还需要考虑以下这种情况，卽对于某些几何問題，并不是要求对于每一次特殊給定的点找出一个作图法，而是要求一个一般的作图法，它(在适当范围之內)总給出問題的解. 从代数的观点来說就是，要給出一个統一的公式(它可以包含二次根式)，它对于在适当范围之內的 $a, b, \cdots$ 的所有的值都給出一个有意义的解 x，它适合这个几何問題的方程. 或者也可以說成，当已知元素 $a, b, \cdots$ 用不定元来代替，决定 x 的方程以及解方程所出現的二次根式等等仍然是有意义的. 譬如說，用圓規与直尺能不能三等分角就是一个这样的問題，利用关系

$$\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi,$$

这个問題可以化成解方程

$$4x^3 - 3x = \alpha \qquad (\alpha = \cos 3\varphi), \tag{1}$$

这个問題并不是說，对于 α 每一个特殊的值用开平方来求方程(1)的一个解，而是問，方程(1)是否有一个解的公式；这个解的公式对于不定元 α 是有意义的.

現在我們已經把用圓規与直尺可构造性的几何問題化为下面

这样一个代数問題：在什么时候元素 x 可以由已知元素 $a, b, \cdots$ 通过有理运算与平方根表示？

这个問題不难回答。 設 $\mathfrak{K}$ 是已知元素 $a, b, \cdots$ 的有理函数域。 假如 x 可以由 $a, b, \cdots$ 經有理运算与平方根表示，那么 x 必然属于一个由 $\mathfrak{K}$ 經过有限多次添加平方根所得的域，这个域也就是經过有限多次 2 次扩张得到的。如果我們在每添加了一个平方根之后就把共軛元素的平方根也添加进去，这些扩张仍然是 2 次的，那么就得到一个次数为 2^m 的正規扩域，它包含 x。 因之：

如果綫段 x 可以用圓規与直尺作出，那么数 x 一定属于 $\mathfrak{K}$ 的一个 2^m 次的正規扩域。

这个条件也是充分的。 因为 2^m 次的域的 Galois 羣是 2^m 阶的，而每个阶为素数冪的羣是可解的（§ 48，习题 5）。 因之有一合成羣列，它的合成因子全是 2 阶的，根据 Galois 理論基本定理与之对应有一域鏈，其中每一个对于前一个都是 2 次的。 2 次扩张总可以由添加一个平方根得出；因而元素 x 可以用平方根表示。 于是結論得証。

对于一些古典的問題我們来应用上面一般的定理。

Deli 的倍立方的問題[1]化成三次方程

$$x^3 = 2,$$

根据 Eisenstein 判別法它是不可約的，因而它的每一个根生成一 3 次扩域，但是这样一个域不可能是 2^m 次域的子域。 因之倍立方的問題不能用圓規与直尺解。

---

1) 关于这些問題的历史我們是从 Archimedeskommentar des Eutokios 知道的。参看 Th. Heath, History of Greek Mathematics I（希腊数学的历史 I），244—270，还有最近的 B. L. van der Waerden, Ontwakende Wetenschap（科学的覺醒），180—185 (Groningen, 1950)。

我們已經看到，三等分角的問題化成方程

$$4x^3 - 3x - \alpha = 0,$$

这里 α 是不定元。这个方程在 α 的有理函数域中的不可約性是容易証明的：假如左端有一个对 α 是有理的因子，那么它一定有对 α 是整有理的因子；但是当 α 的綫性多項式的系数沒有公因子时，它一定是不可約的。于是和上面一样，三等分角不能用圓規与直尺来作。

如果我們在 $\alpha = \cos 3\varphi$ 的有理函数域上再添加元素

$$i \sin 3\varphi = \sqrt{-(1 - \cos^2 3\varphi)},$$

并求

$$y = \cos\varphi + i \sin\varphi$$

的方程，三等分角的方程就具有在代数上更为清楚的形式。事实上

$$(\cos\varphi + i\sin\varphi)^3 = \cos 3\varphi + i \sin 3\varphi,$$

即

$$y^3 = \beta.$$

由复数的几何意义也很容易把角 3φ 的三等分問題化成上面这个純粹方程。

化圓为方归結为数 π 的构造． 如果我們証明了 π 根本不适合任何代数方程，換句話說，它是超越的，那么这个問題的不可能性就証明了；因为 π 不属于有理数域的任何一个有限扩张。至于这个証明，不属于代数的范围，可参看 G. Hessenberg 的书 Transzendenz von e und π（e 与 π 的超越性）。

在給定圓周內正多边形的作图在 h 边形时归結为元素

$$2\cos\frac{2\pi}{h} = \zeta + \zeta^{-1}$$

的构造，其中 ζ 表示 h 次原单位根 $e^{\frac{2\pi i}{h}}$。因为在分圓域的 Galois

羣中只有代换 $\zeta \to \zeta$ 与 $\zeta \to \zeta^{-1}$ 保持这个元素不变，从而它生成一个次数为 $\frac{\varphi(h)}{2}$ 的实子域，所以它的可构造性的条件是：$\frac{\varphi(h)}{2}$，因而也就是 $\varphi(h)$ 是 2 的冪。对于 $h = 2^\nu q_1^{\nu_1}\cdots q_r^{\nu_r}$ (q_i 是奇素数) 有

$$(2) \qquad \varphi(h) = 2^{\nu-1} q_1^{\nu_1-1}\cdots q_r^{\nu_r-1}(q_1-1)\cdots(q_r-1).$$

(在 $\nu = 0$ 的情形第一个因子沒有.)条件就是：奇素数因子在 h 中只能出現一次方 ($\nu_i = 1$) 幷且对于每个在 h 中出現的奇素数 q_i，数 $q_i - 1$ 必須是 2 的冪；这就是說，每个 q_i 必有形式

$$q_i = 2^k + 1.$$

具有这种形式的素数是哪一些?

k 不可能被奇数 $\mu > 1$ 整除，因为由

$$k = \mu\nu, \quad \mu \text{ 奇数}, \quad \mu > 1$$

就要推出，$(2^\nu)^\mu + 1$ 被 $2^\nu + 1$ 整除，于是它不是素数。

因之必有 $k = 2^\lambda$ 与

$$q_i = 2^{2^\lambda} + 1.$$

$\lambda = 0, 1, 2, 3, 4$ 确实給出素数 q_i，即

$$3, 5, 17, 257, 65537.$$

对于 $\lambda = 5$ 以及一些更大的 λ (究竟多少还不知道)，$2^{2^\lambda} + 1$ 不再是素数；例如 $2^{2^5} + 1$ 有因子 641.

如果 h 除去 2 的冪外最后包含素数 3, 5, 17, …的一次冪，那么正 h 边形是可构造的 (Gauss)。我們在 §55 中已經討論了 17 边形的例子。3, 4, 5, 6, 8 与 10 边形的作图法是熟知的；正 7 与 9 边形就不可能作出，因为它們引导到 6 次分圓域的三次子域。

习題. 証明：三次方程

$$x^3 + px + q = 0$$

在不可約情形一定可以經过代換 $x = \beta x'$ (

所以 s_u^{-1} 也把綫性因子 $z-\vartheta$ 变成 F_1 的一个綫性因子，这就是說，s_u^{-1} 从而 s_u 属于 $\mathfrak{g}$. 反之亦然. 因之 Galois 羣与羣 $\mathfrak{g}$ 含有相同的置换，只是把 u 换成 α.

这个决定 Galois 羣的方法不如它的一个推論在实际上更为有用，这个推論是：

設 $\mathfrak{R}$ 是具有单位元素的整环，素因子分解唯一定理在 $\mathfrak{R}$ 中成立. 設 $\mathfrak{p}$ 是 $\mathfrak{R}$ 中一个素理想，$\overline{\mathfrak{R}}=\mathfrak{R}/\mathfrak{p}$ 是同余类环. $\mathfrak{R}$ 与 $\overline{\mathfrak{R}}$ 的商域分別是 Δ 与 $\overline{\Delta}$. $f(x)=x^n+\cdots$ 是 $\mathfrak{R}[x]$ 中一个多項式，$\bar{f}(x)$ 是在同态 $\mathfrak{R}\to\overline{\mathfrak{R}}$ 下与之对应的多項式，假定它們都沒有重根. 于是方程 $\bar{f}=0$ 对于 $\overline{\Delta}$ 的羣 $\bar{\mathfrak{g}}$ (作为根在适当次序下的置换羣)是 $f=0$ 的羣 $\mathfrak{g}$ 的子羣.

証明. 根据 § 26

$$F(z,u)=\prod_{s_u}(z-s_u\vartheta)$$

在 $\Delta[z,u]$ 中的分解 $F_1F_2\cdots F_k$，其中 F_i 是不可約的，可以認为是在 $\mathfrak{R}[z,u]$ 中的，經过同态映射到 $\overline{\mathfrak{R}}[z,u]$ 即得

$$\bar{F}(z,u)=\bar{F}_1\bar{F}_2\cdots\bar{F}_k.$$

因子 $\bar{F}_1,\cdots$ 可能还可以进一步分解. $\mathfrak{g}$ 中置换把 F_1 变到自身，从而把 $\bar{F}_1$ 也变到自身，其余的 u 的置换把 $\bar{F}_1$ 变成 $\bar{F}_2,\cdots,\bar{F}_k$. $\bar{\mathfrak{g}}$ 中置换把 $\bar{F}_1$ 的一个不可約因子变到自身，因而不能把 $\bar{F}_1$ 变成 $\bar{F}_2,\cdots,\bar{F}_k$，只能把 $\bar{F}_1$ 变到自身，这就是說，$\bar{\mathfrak{g}}$ 是 $\mathfrak{g}$ 的子羣.

我們常常应用这条定理来决定羣 $\mathfrak{g}$. 特别地，我們时常是这样选择理想 $\mathfrak{p}$，使多項式 $f(x)$ 模 $\mathfrak{p}$ 可分解，于是 $\bar{f}$ 的羣 $\bar{\mathfrak{g}}$ 就比較容易决定. 譬如說，$\mathfrak{R}$ 是整数环，$\mathfrak{p}=(p)$，p 是素数. 設 $f(x)$ 模 p 后分解成：

$$f(x)\equiv\varphi_1(x)\varphi_2(x)\cdots\varphi_h(x)\quad(p).$$

由此得

$$\bar{f}=\bar{\varphi}_1\bar{\varphi}_2\cdots\bar{\varphi}_h.$$

$\bar{f}(x)$ 的羣 $\bar{\mathfrak{g}}$ 一定是循环的，因为 Galois 域的自同构羣总是循环的(§ 40). 設 $\bar{\mathfrak{g}}$ 的生成置换 s 分解成輪换：

$$(12\cdots j)(j+1\cdots)\cdots.$$

因为羣 $\bar{\mathfrak{g}}$ 的可迁区域恰好与 $\bar{f}$ 的不可約因子对应，所以在輪换 $(12\cdots j)$，$(j+1,\cdots)\cdots$ 中出現的号碼一定恰好分别地与 $\bar{\varphi}_1,\bar{\varphi}_2,\cdots$ 的根相应. 因之一旦知道了 $\varphi_1,\varphi_2,\cdots$ 的次数 $j,k,\cdots$，于是置换 s 的类型就知道了：s 是由一个 j 項，一个 k 項，…輪换組成. 根据上面的定理，在根的适当編号之下 $\bar{\mathfrak{g}}$

是 $\mathfrak{g}$ 的一个子羣，所以 $\mathfrak{g}$ 一定也包含一个相同类型的置換.

例如，假定一个 5 次的整系数多項式模一个素数分解成一个 2 次与一个 3 次不可約因子，那么它的 Galois 羣就包含一个类型为(12)(345)的置換.

例. 給了整系数方程

$$x^5 - x - 1 = 0.$$

模 2 之后，左端分解成

$$(x^2 + x + 1)(x^3 + x + 1).$$

模 3，它是不可約的，否则它就要有一个綫性的或者二次因子，于是它就要与 $x^9 - x$ 有一个公因子（§40，习題 6），因而与 $x^5 - x$ 或者 $x^5 + x$ 有公因子，这显然是不可能的。因之它的羣包含一 5 項輪換与一个乘积 $(ik)(lmn)$。后面这个置換的三次方是 (ik)；用 (12345) 以及它的冪来变換 (ik) 即得一系列对換 (ik)，(kp)，(pq)，(qr)，(ri)，它們合起来生成对称羣。因之羣 $\mathfrak{g}$ 是对称的。

基于下面的定理，我們可以利用上面提到的事实来造任意次数的方程，它的羣是对称的。定理是：如果一个 n 个文字的可迁置換羣包含一个二項輪換与一个 $(n-1)$ 項輪換，那么它就是对称羣。

証明. 設 $n-1$ 項輪換是 $(12\cdots n-1)$。根据可迁性，二項輪換 (ij) 可以变換成 (kn)，这里 k 是 1 到 $n-1$ 中的一个。用 $(12\cdots n-1)$ 以及它的冪来变換 (kn) 就得出 $(1n)$，$(2n)$，$\cdots$，$(n-1\ \ n)$，它們合起来生成对称羣。

为了利用这个定理来造 n 次的 $(n > 3)$、羣为对称的方程，我們首先选取一个模 2 不可約的 n 次多項式 f_1，然后一个多項式 f_2，它模 3 分解成一个 $n-1$ 次与一个綫性不可約因子，最后再取一 n 次多項式 f_3，它模 5 分解成一个二次因子与一个或两个奇次因子(模 5 全是不可約的)。因为模每个素数有任意次的不可約多項式，所以上面这些多項式总能取到(§40，习題 6)。最后选取 f 使

$$f \equiv f_1 \pmod 2,$$
$$f \equiv f_2 \pmod 3,$$
$$f \equiv f_3 \pmod 5,$$

这一定是可能的，譬如，可以取

$$f = -15f_1 + 10f_2 + 6f_3.$$

它的 Galois 羣是可迁的(因为这个多項式模 2 是不可約的)，包含一个类型为

$(12\cdots n-1)$ 的輪换并且包含一个二次輪换与奇項輪换的乘积。把这个乘积乘到适当的奇次方，我們就得到一个純粹的二項輪换，于是按上面的定理它的 Galois 羣是对称的。

用这个方法我們不但能証明具有对称羣的方程的存在，还能进一步得到，在全体系数不超过上界 N 的整系数多項式中，当 N 趋向 ∞ 时，几乎 100% 的羣是对称的。参看 B. L. van der Waerden, *Math. Ann.*, **109** (1931), 13。

是否对于任意給定的置换羣，都存在有理系数多項式以它为羣，这是一个沒有解决的問題；关于这个問題可参看 E. Noether, Gleichungen mit vorgeschriebener Gruppe（具指定的羣的方程），*Math. Ann.*, **78**, 221。

习題。 1. 方程

$$x^4+2x^2+x+3=0$$

的羣是什么(对于有理数域)?

2. 作一个羣为对称羣的 6 次方程。

第八章　无限域扩张

每个域都可由它的素域經过有限的或无限的扩张得到. 在第五章和第七章中我們研究了有限的域扩张，本章中我們要討論无限域扩张. 先討論代数扩张，再討論超越扩张.

所考察的域都是可交换的.

§62. 代数封閉域

一个已給域的各种代数扩域当中，最大的代数扩域，即不能再进一步代数地扩张的域，自然具有重要的意义. 本节中我們将要証明这种扩张的确存在.

为了使得 Ω 是这样一个最大的代数扩域，必要的条件就是 $\Omega[x]$ 中每个多項式都能完全分解成一次因子（不然的話，根据 §35 还可以添加一个次数大于 1 的多項式的零点，将 Ω 作进一步的扩张）. 这个条件同时也是充分的. 事实上，如果 $\Omega[x]$ 中的每个多項式都能分解成一次因子，而 Ω' 是一个代数扩域，则 Ω' 中的每个元素满足 Ω 中的一个方程，因而（当我們把方程的左端分解成一次因子时）满足 Ω 中一个一次方程. 因此这个元素属于 Ω. 这样一来，就有 $\Omega'=\Omega$. 这就是說，Ω 是最大的代数扩域.

由于这个原因，我們定义：

域 Ω 称为一个代数封閉域，如果在 $\Omega[x]$ 中每个多項式都能分解成一次因子.

与此等价的一个定义如下：Ω 称为代数封閉域，如果 $\Omega[x]$ 中

每一不等于常数的多項式在 Ω 中至少有一个零点，因而在 $\Omega[x]$ 至少有一个一次因子.

事实上，如果这一条件成立，那末当我們把一个多項式分解成素因子时，这些素因子只可能是一次的.

§ 70 中将要証明的"代数学基本定理"説明，复数域是一个代数封閉域. 代数封閉域的另外一个例子，就是所有代数的复数(即满足一个以有理数为系数的代数方程的复数)所組成的域. 如果一个复数是一个以代数数为系数的代数方程的根，那末它不仅对代数数域来說是代数的，对有理数域来說也是代数的，因而它本身也是一个代数数.

在本节中我們将要看到，任給一个域 $\mathbf{P}$，可以通过純代数的途径造出一个代数封閉的扩域. 根据 E. Steinitz，我們有下面的.

基本定理. 每个域 $\mathbf{P}$ 有一个代数封閉的代数扩域 Ω，并且这个域在等价扩张的意义下是唯一地确定的，这就是說：$\mathbf{P}$ 的任意两个代数封閉的代数扩域 Ω 和 Ω' 等价.

为了証明这个定理，先要証明几个引理：

引理 1. 設 Ω 是 $\mathbf{P}$ 的一个代数扩域. Ω 为代数封閉域的一个充分条件是：$\mathbf{P}[x]$ 中的每个多項式在 $\Omega[x]$ 中可分解成一次因子.

証明. 設 $f(x)$ 是 $\Omega[x]$ 中的一个多項式. 如果它不能分解成一次因子，那末我們可以添加一个零点 α 而得到一个真括域 Ω'. α 对 Ω 是代数的，而 Ω 对 $\mathbf{P}$ 是代数的，因此 α 对 $\mathbf{P}$ 是代数的. α 必是 $\mathbf{P}[x]$ 中一个多項式 $g(x)$ 的零点. 另一方面，$g(x)$ 在 $\Omega[x]$ 中分解成一个因子，因此 α 必是 $\Omega[x]$ 中一个一次因子的零点，即 α 必属于 Ω，然而这是与所設相违的.

引理 2. 如果域 $\mathbf{P}$ 已按某种方式良序化，那末有一个一意

地可定义的方式可将多項式整环 $\mathbf{P}[x]$ 良序化，使得在这个良序中 $\mathbf{P}$ 恰为一截段。

証明. 我們定义 $\mathbf{P}[x]$ 中多項式 $f(x)$ 的顺序如下：在下面的情况下 $f(x) < g(x)$：

1. $f(x)$ 的次数 $<$ $g(x)$ 的次数；

2. $f(x)$ 的次数 $=$ $g(x)$ 的次数；例如 $f(x) = a_0x^n + \cdots + a_n$，$g(x) = b_0x^n + \cdots + b_n$；同时对某一足数 k 有

$$\begin{cases} a_i = b_i, & \text{当 } i < k \\ a_k < b_k & (\text{在 } \mathbf{P} \text{ 的良序中}). \end{cases}$$

这里，和通常习惯相反，我們賦給多項式 0 以次数 0. 显然，这个定义給出了 $\mathbf{P}[x]$ 中的一个顺序. 至于它是一个良序这一点，可以証明如下：每个非空的多項式集合中，次数最低的多項式組成一个非空子集. 設这一最低次数为 n. 在这个子集中，首項系数 a_0 在 $\mathbf{P}$ 的良序中出现最早的多項式又成一非空子集；而在后一子集中，具有最早系数 a_1 的多項式又成一非空子集. 余此类推. 最后得到的，具有最早系数 a_n 的多項式的子集只可能包含一个多項式（因为 $a_0, \cdots, a_n$ 由历次的最小性要求所唯一确定），这个多項式就是所給集合中的第一个多項式.

引理 3. 假設域 $\mathbf{P}$ 已經良序化，并且假設給定了一个 n 次多項式 $f(x)$ 和 n 个符号 $\alpha_1, \alpha_2, \cdots, \alpha_n$，那末可以一意地造出一个域 $\mathbf{P}(\alpha_1, \alpha_2, \cdots, \alpha_n)$，并将其良序化，使得 $f(x)$ 在这个域中可以完全分解成一次因子 $\prod_1^n (x - \alpha_i)$，而 $\mathbf{P}$ 在这个域的良序中恰是一个截段.

証明. 我們由 $\mathbf{P} = \mathbf{P}_0$ 出发依次添加根 $\alpha_1, \alpha_2, \cdots, \alpha_n$，从而依次造出域 $\mathbf{P}_1, \mathbf{P}_2, \cdots, \mathbf{P}_n$. 假設域 $\mathbf{P}_{i-1} = \mathbf{P}(\alpha_1, \cdots, \alpha_{i-1})$ 已

經造出且已良序化，使得 $\mathbf{P}$ 是 $\mathbf{P}_{i-1}$ 中的一个截段。 域 $\mathbf{P}_i$ 可按下述方式造出：

首先，根据引理 2，可以将多項式整环 $\mathbf{P}_{i-1}[x]$ 良序化。 在这个整环中，多項式 $f(x)$ 将分解成一些不可約因子的乘积，其中可能包括若干个一次因子 $x-\alpha_1, x-\alpha_2, \cdots, x-\alpha_{i-1}$. 在其余的因子当中，假設 $f_i(x)$ 是在 $\mathbf{P}_{i-1}[x]$ 中的良序下的第一个多項式. 根据 § 35，我們可以把 α_i 作为 $f_i(x)$ 的一个根的符号，从而作出域 $\mathbf{P}_i=\mathbf{P}_{i-1}(\alpha_i)$. 这个域就是所有和

$$\sum_{0}^{h-1} c_\lambda \alpha_i^\lambda$$

的全体，其中 h 是多項式 $f_i(x)$ 的次数。 如果 $f_i(x)$ 是一次的，那末自然就有 $\mathbf{P}_i=\mathbf{P}_{i-1}$，这时 α_i 就不是一个新的符号，而是 $f_i(x)$ 在 $\mathbf{P}_{i-1}$ 中的一个零点. 域 $\mathbf{P}_i$ 可按照下面的定則良序化：对每个域元素 $\sum\limits_{0}^{h-1} c_\lambda \alpha_i^\lambda$，我們使一个多項式 $\sum\limits_{0}^{h-1} c_\lambda x^\lambda$ 与之相对应，并将域中的元素和相应的多項式一样編序。

显然，$\mathbf{P}_{i-1}$ 是 $\mathbf{P}_i$ 的一个截段，因而 $\mathbf{P}$ 也是 $\mathbf{P}_i$ 的一个截段.

这样，我們就依次地造出了域 $\mathbf{P}_1, \mathbf{P}_2, \cdots, \mathbf{P}_n$，并在它們之中定义了良序. $\mathbf{P}_n$ 就是所要求的一意地可定义的域 $\mathbf{P}(\alpha_1, \alpha_2, \cdots, \alpha_n)$.

引理 4. 如果在一个由域所构成的有序集合中，每一个出現在前面的域是每一个出現在后面的域的子域，那末这些域的并集仍是一个域.

証明. 任給并集中的两个元素 α 和 β，可以找到两个域 Σ_α 和 Σ_β 分别包含 α 和 β，其中一个域包含在另一个域之内. 在較大的那个域中 $\alpha+\beta$ 和 $\alpha\cdot\beta$ 都有定义，并且这一定义对上述集合中所有包含 α 和 β 的域都是一样，因为任意两个这样的域中必有一个域是另一域的子域. 現在假設要証明結合律：

$$\alpha\beta\cdot\gamma=\alpha\cdot\beta\gamma.$$

我們从域 Σ_α, Σ_β, Σ_γ 中取最大（出現最晚）的一个，那末 α, β 和 γ 都包含在这个域内，而在这个域中結合律是成立的. 所有其余的运算規律都可以照这一方式来証明.

基本定理的証明可分为两个部分：域 Ω 的作法及其唯一性的証明. 域 Ω 的作法及唯一性的証明都是通过 § 8 中所述的超限归納法来进行的.

Ω 的作法. 引理 1 告訴我們，为了作出 $\mathbf{P}$ 的一个代数封閉的扩域 Ω，只須作出一个对 $\mathbf{P}$ 为代数的域，使得 $\mathbf{P}[x]$ 中所有的多項式都能在这个域中完全分解成一次因子卽可.

我們設想域 $\mathbf{P}$，从而多項式整环 $\mathbf{P}[x]$，已經良序化. 对每个多項式 $f(x)$，我們使一組新的符号 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 与之相对应，后者的个数等于多項式的次数.

对每个多項式 $f(x)$ 可作出两个良序化的域 $\mathbf{P}_f$ 和 Σ_f，这两个域由下面的递归关系定义.

1. $\mathbf{P}_f$ 是域 $\mathbf{P}$ 和所有 $\Sigma_g(g<f)$ 的并集.

2. $\mathbf{P}_f$ 中的良序应該如此确定，以使得 $\mathbf{P}$ 和所有的 $\Sigma_g(g<f)$ 都是 $\mathbf{P}_f$ 的截段.

3. Σ_f 可按引理 3 的作法将符号 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 添加于 $\mathbf{P}_f$ 得出.

現在要証明的是：当所有 $\mathbf{P}_g$, $\Sigma_g(g<f)$ 均已造出，并满足上述要求时，通过上述要求的确能够一意地确定两个良序化的域 $\mathbf{P}_f$ 和 Σ_f.

如果 3. 成立，那末首先可以断定 $\mathbf{P}_f$ 是 Σ_f 的一个截段. 由这一事实，并由 2. 可以推知，$\mathbf{P}$ 和每个 $\Sigma_g(g<f)$ 都是 Σ_f 的截段. 假設对所有先于 f 的足标这三个要求都已满足，則

$$\begin{cases}\text{对任意 } h < f,\ \mathbf{P} \text{ 是 } \Sigma_h \text{ 的截段;}\\ \text{对任意 } g < h < f,\ \Sigma_g \text{ 是 } \Sigma_h \text{ 的截段.}\end{cases}$$

由此可知，域 $\mathbf{P}$ 和 $\Sigma_h(h < f)$ 組成一个引理 4 所要求的有序集合，因而它們的并集仍是一个域。这个域就是相应于条件 1 的域 $\mathbf{P}_f$。$\mathbf{P}_f$ 中的良序由条件 2 所唯一确定。事实上，$\mathbf{P}_f$ 中的任意两个元素 a 和 b 必属于 $\mathbf{P}$ 或某一 Σ_g，在那里它們之間有順序 $a < b$ 或 $a > b$，这一順序在 $\mathbf{P}_f$ 的良序中应該保持不变。这一順序对所有包含 a 和 b 的域 $\mathbf{P}$ 或 Σ_g 都是一样的，因为所有这些域中一个是另一个的截段。这样就的确在 $\mathbf{P}_f$ 中定义了一个順序。至于这个順序是一个良序，这一点也是显然的。事实上，$\mathbf{P}_f$ 中的一个非空集 $\mathfrak{M}$ 至少包含 $\mathbf{P}$ 或某一 Σ_g 中的一个元素，因而包含一个属于 $\mathbf{P}$ 或 Σ_g 的最早的元素。这个元素就是 $\mathfrak{M}$ 中的第一个元素。

这样一来，域 $\mathbf{P}_f$ 以及其中的良序就由条件 1. 和 2. 所唯一地确定了。由于 Σ_f 可由条件 3 唯一确定，故 $\mathbf{P}_f$ 和 Σ_f 都造出来了。

由于条件 3. 多項式 f 在 Σ_f 中可完全分解成一次因子。其次，我們可以用超限归納法証明，Σ_f 对 $\mathbf{P}$ 是代数的。事实上，假設所有 $\Sigma_g(g < f)$ 都是代数的，那末这些域和 $\mathbf{P}$ 的并集，即域 $\mathbf{P}_f$ 也是代数的。另一方面，根据条件 3. Σ_f 对 $\mathbf{P}_f$ 是代数的，故对 $\mathbf{P}$ 也是代数的。

最后，我們作所有 Σ_f 的并集 Ω。根据引理 4，这个并集仍是一个域，这个域对 $\mathbf{P}$ 是代数的，并且在它里面所有多項式 f 都能完全分解成一次因子（因为每个 f 在 Σ_f 中已能分解成一次因子）；这样，域 Ω 就是代数封閉的（引理 1）。

Ω 的唯一性. 現在假設 Ω 和 Ω' 是两个域，二者都是代数封閉的，并且对 $\mathbf{P}$ 是代数的，我們要証明它們的等价性。为了这个

目的，我們假設两个域都已良序化．对Ω的每个截段$\mathfrak{A}$（这里Ω本身也算作截段之一），我們要作出Ω'的一个截段$\mathfrak{A}'$和一个同构

$$\mathbf{P}(\mathfrak{A}) \cong \mathbf{P}(\mathfrak{A}').$$

这一同构应满足下面的递归条件．

1. 同构$\mathbf{P}(\mathfrak{A}) \cong \mathbf{P}(\mathfrak{A}')$使得域$\mathbf{P}$中的元素不动．

2. 对$\mathfrak{B} \subset \mathfrak{A}$，同构$\mathbf{P}(\mathfrak{A}) \cong \mathbf{P}(\mathfrak{A}')$是$\mathbf{P}(\mathfrak{B}) \cong \mathbf{P}(\mathfrak{B}')$的一个开拓．

3. 如果$\mathfrak{A}$有一个最末元素a，从而$\mathfrak{A} = \mathfrak{B}' \vee \{a\}$，并且$a$是$\mathbf{P}(\mathfrak{B})$中一个不可約多項式$f(x)$的根，而$f'(x)$是在同构$\mathbf{P}(\mathfrak{B}) \cong \mathbf{P}(\mathfrak{B}')$下和$f(x)$对应的多項式，則$a'$是$f'(x)$在$\Omega'$的良序中的一个根．

現在須要証明的是：如果对所有較$\mathfrak{A}$为先的截段$\mathfrak{B} \subset \mathfrak{A}$满足上述条件的同构已經造出，那末这三个条件的确能够决定一个，而且是唯一的一个同构$\mathbf{P}(\mathfrak{A}) \cong \mathbf{P}(\mathfrak{A}')$．下面我們要区分两种不同的情形．

第一种情形．$\mathfrak{A}$中沒有最末元素．这时$\mathfrak{A}$的每个元素a都已包含在一个較先的截段$\mathfrak{B}$之內，这就是說，$\mathfrak{A}$是所有$\mathfrak{B}$（$\mathfrak{B} \subset \mathfrak{A}$）的并集，因而$\mathbf{P}(\mathfrak{A})$是域$\mathbf{P}(\mathfrak{B})$的并集．由于每个同构$\mathbf{P}(\mathfrak{B}) \cong \mathbf{P}(\mathfrak{B}')$都是較先的同构的开拓，每个元素$\alpha$在所有这些同构之下被映成同一元素$\alpha'$．因此，我們能够找到一个，而且仅能找到一个同构$\mathbf{P}(\mathfrak{A}) \to \mathbf{P}(\mathfrak{A}')$，使得它包含所有較先的同构$\mathbf{P}(\mathfrak{B}) \to \mathbf{P}(\mathfrak{B}')$，这个同构就是对应$\alpha \to \alpha'$．这个对应显然是一个1-同构，并满足条件1．和2．

第二种情形．$\mathfrak{A}$中有一个最末元素a．这时$\mathfrak{A} = \mathfrak{B} \vee \{a\}$．条件1．一意地确定了和$a$对应的元素$a'$．由于$a'$所满足的$\mathbf{P}(\mathfrak{B}')$中的不可約方程和$a$所满足的$\mathbf{P}(\mathfrak{B})$中的不可約方程是（在同构意

义下的)"同一个"方程，故同构 $\mathbf{P}(\mathfrak{B}) \to \mathbf{P}(\mathfrak{B}')$ (当 $\mathfrak{B}$ 为空集时就是恆等同构 $\mathbf{P} \to \mathbf{P}$) 可开拓为一个同构 $\mathbf{P}(\mathfrak{B}, a) \to \mathbf{P}(\mathfrak{B}', a')$，其中 a 被映射成 a' (§ 38). 这一同构由条件 3. 唯一确定；因为每个系数属于 $\mathbf{P}(\mathfrak{B})$ 的有理函数 $\varphi(a)$ 必須映成以 $\mathbf{P}(\mathfrak{B}')$ 中相应元素为系数的有理函数. 这样构出的同构显然满足条件 1. 和 2.

这样一来，同构 $\mathbf{P}(\mathfrak{A}) \to \mathbf{P}(\mathfrak{A}')$ 就作出来了. 如命 Ω'' 表示所有 $\mathbf{P}(\mathfrak{A}')$ 的并集，那末就有一个同构 $\mathbf{P}(\Omega) \to \Omega''$ 或 $\Omega \to \Omega''$，它使得 $\mathbf{P}$ 按元素不动. 由于 Ω 是代数封閉的，Ω'' 也应是代数封閉的，因而 Ω'' 应和整个 Ω' 相重合. 从这里就得出了曾經断言过的 Ω 和 Ω' 的等价性.

一个已給域的代数封閉扩域之所以有意义，在于这个扩域在扩张的等价性的意义之下包含了一切可能代数扩域. 更确切地說：

如果 Ω 是域 $\mathbf{P}$ 的一个代数封閉的代数扩域，而 Σ 是 $\mathbf{P}$ 的任意代数扩域，那末在 Ω 內可以找到一个和 Σ 等价的扩域 Σ_0.

証明. 我們可以把 Σ 扩成一个代数封閉的代数扩域 Ω'. 这个域对 $\mathbf{P}$ 来說也是代数的，因而与 Ω 等价. 把 Ω' 映射成 Ω 并使得 $\mathbf{P}$ 按元素不动的同构，特别将 Σ 映射成 Ω 中的一个等价子域 Σ_0.

习题. 証明：任給 $\mathbf{P}[x]$ 中的一組多項式，存在 $\mathbf{P}$ 的一个唯一的扩张域 Ω，这个域是通过添加这組多項式的一切零点而得的.

附註. 我們也可以在本节定理的証明中用 Zorn 的一条引理来代替超限归納法. 为了明白地陈述这条引理，我們先得引进几个預备概念.

一个集合 M 的一些子集的一个集合 K 称为一个鏈，如果对于 K 中任意两个集合总有一个包在另一个里. M 的一些子集的一个集合 A 称为閉的，如果在它包有一个鏈中的集合的同时，也包有它們的并集.

那么 Zorn 引理可以說成：M 的一些子集的一个閉集合 A 总包有一个极大元素，即这样的一个元素，它不是 A 中另外元素的子集.

見 M. Zorn, *Bull. Amer. Math. Soc.*, 41 (1935), 667.

§63. 单純超越扩域

我們知道，一个（交换）域Δ的每个单純超越扩域都等价于多項式整环$\Delta[x]$的商域$\Delta(x)$。由此之故，我們要对这个商域

$$\Omega = \Delta(x)$$

进行研究。Ω中的元素即有理函数

$$\eta = \frac{f(x)}{g(x)}.$$

我們可以假定每个这样的分式都是不可約的（即 f 和 g 无公因子）。$f(x)$ 和 $g(x)$ 的次数中的最大者称为函数 η 的次数。

定理. 每个次数为 n 的不等于常数的 η 对Δ是超越的，而 $\Delta(x)$ 对 $\Delta(\eta)$ 是代数的，其次数为 n。

証明. 設表式 $\eta = f(x)/g(x)$ 是不可約的。这时 x 滿足方程

$$g(x)\eta - f(x) = 0,$$

方程的系数属于$\Delta(\eta)$。这些系数不可能全等于零。事实上，如果这个方程所有系数都等于零，而 a_k 是 $g(x)$ 中一个不等于零的系数，b_k 是 $f(x)$ 中 x 的同次冪的系数，那末我們就会得到

$$a_k\eta - b_k = 0,$$

从而有 $\eta = b_k/a_k =$ 常数，与所設相违。由此可知，x 对 $\Delta(\eta)$ 是代数的。

如果 η 对Δ是代数的，那末 x 对Δ也会是代数的，但实际情形不是这样。因此 η 是超越的。

x 是 $\Delta(\eta)[z]$ 中一个 n 次多項式

$$g(z)\eta - f(z)$$

的零点。这个多項式在$\Delta(\eta)[z]$中是不可約的。不然的話，根据

§ 26，它在 $\Delta[\eta, z]$ 中也将是可約的． 但这个多項式对 η 来說是一次的，其中必有一个因子不依賴于 η 而仅依賴于 z． 由于 $g(z)$ 和 $f(z)$ 无公因子，这样一个因子是不可能存在的．

这样一来，x 对 $\Delta(\eta)$ 就是一个次数为 n 的代数元素． 由此即得断言 $(\Delta(x):\Delta(\eta)) = n$．

为了下面的需要，我們在这里指出，多項式

$$g(z)\eta - f(z)$$

沒有仅仅依賴于 z 的（即位于 $\Delta[z]$ 內的）因子． 当我們把 η 代以它的値 $f(x)/g(x)$ 并将整个式子乘以分母 $g(x)$ 时，这一事也仍然成立． 这就是說，$\Delta[x, z]$ 中的多項式

$$g(z)f(x) - f(z)g(x)$$

沒有仅依賴于 z 的因子．

由上面証明的定理可得出三个推論：

1．一个函数 $\eta = f(x)/g(x)$ 的次数仅取决于域 $\Delta(\eta)$ 和 $\Delta(x)$，而与后一域的生成元 x 的特殊选擇无关．

2． $\Delta(\eta) = \Delta(x)$，当且仅当 η 的次数为 1，即 η 为分式綫性函数． 这就是說，可作为域 $\Delta(x)$ 的生成元的，除了 x 之外还有 x 的所有分式綫性函数，并且仅有这些函数．

3． $\Delta(x)$ 的任何一个使得 Δ 中的元素不动的自同构必将 x 映成另一生成元． 反之，如果我們将 x 映成域的另一生成元 $\bar{x} = \dfrac{ax+b}{cx+d}$，而将每一 $\varphi(x)$ 映成 $\varphi(\bar{x})$，那末就可以得到一个自同构，这个自同构使得 Δ 中的元素不动．

$\Delta(x)$ 相对于 Δ 的全部自同构，就是分式綫性代換

$$\bar{x} = \frac{ax+b}{cx+d}, \quad ad - bc \neq 0.$$

对于某些几何学上的应用来說，下面的定理具有重要意义．

Lüroth 定理. 每个中間域Σ：$\Delta \subset \Sigma \subseteq \Delta(x)$，都是一个单純超越扩域：$\Sigma = \Delta(\vartheta)$.

証明. 元素x对域Σ来說必是代数的. 事实上，假設η是Σ中任意一个不属于Δ的元素，那末象上面已經証明过的那样，x对$\Delta(\eta)$是代数的，对整个Σ来說更应当是如此. 現設多項式整环$\Sigma[z]$中首項系数为1且以x为零点的不可約多項式是

(1) $$f_0(z) = z^n + a_1 z^{n-1} + \cdots + a_n.$$

我們要决定这个多項式$f_0(z)$的构造.

系数a_i是x的有理函数. 乘上公分母之后可以使得这些系数都是整有理函数，并且可以作到使所得的多項式

$$f(x, z) = b_0(x)z^n + b_1(x)z^{n-1} + \cdots + b_n(x)$$

对x来說是一个本原多項式. 設这个多項式对x的次数是m，对z的次数是n.

(1) 的系数$a_i = b_i/b_0$不可能全都和x无关，因为不然的話x就会是Δ上的一个代数元素. 因此必有一个系数，譬如說

$$\vartheta = a_i = \frac{b_i(x)}{b_0(x)},$$

或者写成不可約形式时，

$$\vartheta = \frac{g(x)}{h(x)}$$

是的确和x有关的. $g(x)$和$h(x)$的次数都不大于m. 多項式(不为零的)

$$g(z) - \vartheta h(z) = g(z) - \frac{g(x)}{h(x)} h(z)$$

有零点$z = x$，因而在$\Sigma[z]$中可被$f_0(z)$整除. 根据 § 26，当我們把这两个对x为有理的多項式整理成对x为整有理的本原多項式时，这一可除性仍然成立. 这样我們就有

$$h(x)g(z) - g(x)h(z) = q(x, z)f(x, z).$$

左端对 x 的次数不超过 m，而右端的因子 f 就已經是 m 次的，由此可知右端的次数应該恰等于 m，从而 $q(x, z)$ 与 x 无关．另一方面，左端不可能有一个仅和 z 有关的因子，因此 $q(x, z)$ 应是一个常数：

$$h(x)g(z) - g(x)h(z) = q \cdot f(x, z).$$

这样一来，由于常数 q 不起影响，$f(x, z)$ 的构造就决定了．$f(x,z)$ 对 x 的次数是 m，因此（根据对称性）它对 z 的次数也是 m．由此即得 $m = n$．$g(x)$ 和 $h(x)$ 的次数当中至少有一个达到最大值 m，因此 ϑ 作为 x 的有理函数来看，其次数恰等于 m．

这样一来，一方面有

$$(\Delta(x):\Delta(\vartheta)) = m,$$

另一方面有

$$(\Delta(x):\Sigma) = m.$$

由于 Σ 包含着 $\Delta(\vartheta)$，故有

$$(\Sigma:\Delta(\vartheta)) = 1,$$

即

$$\Sigma = \Delta(\vartheta).$$

Lüroth 定理在几何学中有下面的意义：

一条（不可約的）平面曲綫 $F(\xi, \eta) = 0$ 称为一条**有理曲綫**，如果它上面的点除有限多个之外可由有理的参数方程：

$$\xi = f(t),$$
$$\eta = g(t)$$

来表示．

可能出現这样一种情况，即曲綫上的每个点（可能要除去其中有限多个）都相当于 t 的好几个值（例如当

$$\xi = t^2,$$
$$\eta = t^2 + 1$$

时，相当于 t 和 $-t$ 的是同一个点）． 根据 Lüroth 定理，我們可以适当地选择参数而避免这样的情况．設 Δ 是一个域，函数 f 和 g 的系数是属于这个域的，再設 t 是一个未定元．$\Sigma=\Delta(f,g)$ 是 $\Delta(t)$ 的一个子域．如果 t' 是 Σ 的一个本原元素，則有

$$f(t)=f_1(t') \qquad (\text{有理函数}),$$
$$g(t)=g_1(t') \qquad (\text{有理函数}),$$
$$t'=\varphi(f,g)=\varphi(\xi,\eta).$$

容易驗証新的参变数

$$\xi=f_1(t'),$$
$$\eta=g_1(t')$$

表示同一曲綫，而函数 $\varphi(x,y)$ 的分母只在曲綫上的某有限个点为零，因此对曲綫上的每个点（除有限多个点之外）只有 t' 的一个值与之相当．

习題． 如果域 $\Delta(x)$ 对子域 $\Delta(\eta)$ 是正規的，則多項式 (1) 在它里面完全分解为一次因子． 所有这些因子都可以由其中的一个，例如由 $z-x$，对 x 作分式綫性变換得出．这些分式綫性变換組成一个有限羣，它們使得函数 $\vartheta=g(x)/h(x)$ 不变，并且可由这一性質来刻划．

§64. 代数相关性与无关性

設 Ω 是某一固定的域 $\mathbf{P}$ 的一个扩域． 我們説 Ω 中的一个元素 v 和 $u_1,\cdots,u_n$ 代数相关，如果 v 对域 $\mathbf{P}(u_1,\cdots,u_n)$ 来説是代数的，卽 v 滿足一个代数方程

$$a_0(u)v^g+a_1(u)v^{g-1}+\cdots+a_g(u)=0,$$

其中的系数 $a_0(u),\cdots,a_g(u)$ 是 $u_1,\cdots,u_n$ 的系数属于 $\mathbf{P}$ 的多項式，且不全为零．

代数相关这一关系具有下面的基本性質，这些性質和綫性相关性的基本性質完全类似（参看 §36）：

基础定理 1． 每个 $u_i(i=1,\cdots,n)$ 都和 $u_1,\cdots,u_n$ 代数相关．

基础定理 2． 如果 v 和 $u_1,\cdots,u_n$ 代数相关，而不和 u_1，

$\cdots, u_{n-1}$ 代数相关，则 u_n 和 $u_1, \cdots, u_{n-1}, v$ 代数相关.

証明. 我們設想已經把 $u_1, \cdots, u_{n-1}$ 添加到基域上去了. 这时 v 就和 u_n 代数相关，因而有一个代数关系式

(1) $$a_0(u_n)v^g + a_1(u_n)v^{g-1} + \cdots + a_g(u_n) = 0.$$

将这个方程按 u_n 的升冪排列，就得

(2) $$b_0(v)u_n^h + b_1(v)u_n^{h-1} + \cdots + b_g(v) = 0.$$

据假設，v 对基域 $\mathbf{P}(u_1, \cdots, u_{n-1})$ 是超越的. 因此，$b_0(v), b_1(v), \cdots, b_n(v)$ 或者恆等于零(作为 v 的多項式来看)，或者 $\neq 0$. 但这些多項式不可能全恆等于零的多項式，因为不然的話，(1)的左端作为 v 的多項式也将恆等于零，卽有 $a_0(u_n) = a_1(u_n) = \cdots = a_n(u_n) = 0$，而这是与所設相违的. 这样，在 (2) 中不可能所有的系数 b_k 都等于零. 因此，由于 (2)，u_n 相对于基域 $\mathbf{P}(u_1, \cdots, u_{n-1})$ 来說，和 v 代数相关.

基础定理 3. 設 w 和 $v_1, \cdots, v_s$ 代数相关，而每个 $v_j (j = 1, \cdots, s)$ 又和 $u_1, \cdots, u_n$ 代数相关，则 w 和 $u_1, \cdots, u_n$ 代数相关.

証明. 如果 w 对域 $\mathbf{P}(v_1, \cdots, v_n)$，从而对域 $\mathbf{P}(u_1, \cdots, u_n, v_1, \cdots, v_n)$ 来說是代数的，而后一域对 $\mathbf{P}(u_1, \cdots, u_n)$ 是代数的，則根据 § 38，w 对 $\mathbf{P}(u_1, \cdots, u_n)$ 也是代数的. 这就是所要証明的.

由于綫性相关性的几个基础定理現在都能成立，故 § 36 中所建立的其它导出定理，特别是替換定理，也同样能成立.

类似于綫性无关性的概念，現在我們可以引进代数无关性的概念：$u_1, \cdots, u_r$ 称为对基域 $\mathbf{K}$ 代数无关，如果沒有一个 u_i 和其余元素 u_j 代数相关. 我們有

定理. 元素 $u_1, \cdots, u_r$ 代数无关的充分必要条件，是由

$$f(u_1, \cdots, u_r) = 0,$$

其中 f 是系数属于 $\mathbf{P}$ 的多項式，必然地可以推出这个多項式的系数全等于零。

証明。 如果由 $f(u_1, \cdots, u_r)=0$ 即可推出这个多項式恆等于零，那末显然沒有一个 u_i 和其余的 u_j 代数相关。現在反过来假設 $u_1, \cdots, u_r$ 代数无关。設

$$f(u_1, \cdots, u_r)=0,$$

并将多項式 f 按 u_r 的冪排列，則这个多項式的系数 $f_i(u_1, \cdots, u_{r-1})$ 都将等于零。再将这些多項式按 u_{r-1} 的冪排列，并用同样的方式来进行推論，最后可知多項式 f 所有的系数都应等于零。

根据这个定理可知，如果 $u_1, u_2, \cdots, u_n$ 代数无关的話，它們不能由任何代数方程彼此相关联。因此这些元素也称为无关超越元素。

如果 $u_1, \cdots, u_r$ 对 $\mathbf{P}$ 是代数无关的，而 $z_1, \cdots, z_r$ 是一組不定元，那末每个系数属于 $\mathbf{P}$ 的多項式 $f(z_1, \cdots, z_r)$ 都有一个多項式 $f(u_1, \cdots, u_n)$ 与之双方单值地相对应。因此，$\mathbf{P}[z_1, \cdots, z_r] \cong \mathbf{P}[u_1, \cdots, u_r]$。由多項式环的同构可得出其商域的同构：

$$\mathbf{P}(z_1, \cdots, z_r) \cong \mathbf{P}(u_1, \cdots, u_r).$$

因此，无关超越元素 $u_1, \cdots, u_r$ 在所有代数性質上和不定元一致。

代数相关与代数无关的概念也可以对无限集合来定义。

我們說元素 v（对基域 $\mathbf{P}$）和集合 $\mathfrak{M}$（代数）相关，如果它对域 $\mathbf{P}(\mathfrak{M})$ 是代数的，即这个元素能够滿足一个代数方程，而这个方程的系数是 $\mathfrak{M}$ 中的元素的有理函数（系数属于 $\mathbf{P}$）[1]。在这一情况下，我們可以将方程乘以系数的分母的积，使之对 $\mathfrak{M}$ 中的元素来說是有理整的。由于在这样一个方程中只出現 $\mathfrak{M}$ 中的有限多个元素

---

1) 如果一个元素对 $\mathbf{P}$ 是代数的，我們就說它和空集代数相关。

$u_1, \cdots, u_n$，故有下面的結論：

如果 v 和 $\mathfrak{M}$ 代数相关，則 v 必和 $\mathfrak{M}$ 中某有限多个元素代数相关。

如果我們这样地选择有限子集 $\{u_1, \cdots, u_n\}$，使得其中沒有一个元素是多余的，那末根据基础定理 2，每一 u_i 和 v 以及其余的 u_j 代数相关。

基础定理 3 可以直接推广到无限集合：

如果 u 和 $\mathfrak{M}$ 代数相关，而 $\mathfrak{M}$ 中的每个元素又和 $\mathfrak{N}$ 代数相关，則 u 和 $\mathfrak{N}$ 代数相关。

我們說一个集合 $\mathfrak{N}$ 和一个集合 $\mathfrak{M}$（代数）相关，如果 $\mathfrak{N}$ 中所有的元素都和 $\mathfrak{M}$ 代数相关。 如果 $\mathfrak{N}$ 和 $\mathfrak{M}$ 相关，而 $\mathfrak{M}$ 又和 $\mathfrak{L}$ 相关，則 $\mathfrak{N}$ 和 $\mathfrak{L}$ 相关。

如果两个集 $\mathfrak{M}$ 和 $\mathfrak{N}$ 彼此代数相关，我們就說他們（对基域 **P**）等价。等价关系是自反的、对称的和传递的。

一个集合 $\mathfrak{M}$ 称为（对域 **P**）不可約或代数无关的，如果 $\mathfrak{M}$ 中沒有一个元素和其余的元素代数相关。 在这一情形下我們也說，集合 $\mathfrak{M}$“完全由代数无关元素組成”。

如果 $\mathfrak{M}$ 是不可約的，那末 $\mathfrak{M}$ 中有限多个不同元素之間的一个关系

$$f(u_1, \cdots, u_r) = 0$$

（其中 f 是系数在 **P** 中的多項式）只有当 f 恆等于零，即

$$f(x_1, \cdots, x_r) = 0 \qquad (\text{对不定元 } x_i)$$

时才能成立。

現在如果我們作一个多項式整环 $\mathbf{P}[\mathfrak{X}]$，其不定元的个数和 $\mathfrak{M}$ 中元素的个数一样（有限或无限多个）。对每个元素 $f(x_1, \cdots, x_r)$ 我們使域元素 $f(u_1, \cdots, u_r)$ 与之相对应。 这样显然得出多項式

整环到由域元素 $f(u_1, \cdots, u_r)$ 所組成的集合 $\mathbf{P}[\mathfrak{M}]$ 的一个同态。另一方面，如果 $\mathfrak{M}$ 是不可約的，則这个同态把不同的多項式映成不同的域元素，因而在这一情形下我們有 1-同构：

$$\mathbf{P}[\mathfrak{X}] \cong \mathbf{P}[\mathfrak{M}].$$

由多項式环的同构又可以得出其商域的同构。这就証明了下面的結論：

将一个代数无关的集添加到 $\mathbf{P}$ 所得的域 $\mathbf{P}(\mathfrak{M})$ 同构于一个和 $\mathfrak{M}$ 等势的不定元的集合 $\mathfrak{X}$ 的有理函数域，即多項式整环 $\mathbf{P}[\mathfrak{X}]$ 的商域。

将一个代数无关集合 $\mathfrak{M}$ 添加于 $\mathbf{P}$ 而得的任何一个域 $\mathbf{P}(\mathfrak{M})$ 称为 $\mathbf{P}$ 的一个**純超越扩张**。純超越扩张的結构由前面的定理完全确定：每个这样的域都同构于一个多項式整环的商域。因此，这种域的結构只和不可約集合 $\mathfrak{M}$ 的势有关。这个势就是下一节所要討論的**超越次数**。

§ 65. 超越次数

我們要証明，每个域扩张都可以分解成一个純超越扩张和这一純超越扩张之上的一个代数扩张。这个結論要归根于下面这样一个定理：

如果 Ω 是 $\mathbf{P}$ 的一个扩张，則 Ω 中的每个子集 $\mathfrak{M}$ 和一个包含在它之內的不可約集合 $\mathfrak{M}'$ 等价。

証明。 設 $\mathfrak{M}$ 已經良序化。子集 $\mathfrak{M}'$ 的定义如下：$\mathfrak{M}$ 中的一个元素 a 属于 $\mathfrak{M}'$，如果它和位于它之前的截段 $\mathfrak{A}$ 无关［因而对 $\mathbf{P}(\mathfrak{A})$ 是超越的］。关于 $\mathfrak{M}'$，下面的事实成立：

1. $\mathfrak{M}'$ 是不可約的。事实上，如果某一元素，譬如設 a_1，和元素 $a_2, \cdots, a_k$ 相关，我們設集合 $\{a_2, \cdots, a_n\}$ 是一个最小的这样

的集合．这时a_i当中的每一个都和其余的相关．特别，在 $\mathfrak{M}$ 中的良序下居最末的元素 a_i 和所有属于它之前的其余元素相关．根据 $\mathfrak{M}'$ 的定义，这个最末元素 a_i 不可能属于 $\mathfrak{M}'$．

2．$\mathfrak{M}$ 和 $\mathfrak{M}'$ 相关．不然的話，$\mathfrak{M}$ 中和 $\mathfrak{M}'$ 不相关的元素当中有一个最先的元素 a．a 不属于 $\mathfrak{M}'$，因而必和位于它之前的截段 $\mathfrak{A}$ 相关，而这个截段本身是和 $\mathfrak{M}'$ 相关的（因为 a 是第一个不和 $\mathfrak{M}'$ 相关的元素）．因此 a 和 $\mathfrak{M}'$ 相关，而这是与所設相违的．

推論． 如果 $\mathfrak{M} \subseteq \mathfrak{N}$，則 $\mathfrak{M}$ 中的每一个和 $\mathfrak{M}$ 等价的不可約子集 $\mathfrak{M}'$ 可扩充为 $\mathfrak{N}$ 中一个和 $\mathfrak{N}$ 等价的不可約子集 $\mathfrak{N}'$．

証明．在 $\mathfrak{N}$ 中引入一个良序，使得在这个良序中 $\mathfrak{M}$ 中的元素居于最前，并在 $\mathfrak{N}$ 中作出相应的子集 $\mathfrak{N}'$，其作法和上面在 $\mathfrak{M}$ 中作子集 $\mathfrak{M}'$ 一样．这样一来，$\mathfrak{N}'$ 显然包含着 $\mathfrak{M}'$ 中的元素．

从上面的定理可以看出，$\mathbf{P}$ 的每一个扩张都可以看作是 $\mathbf{P}(\mathfrak{S})$ 的一个代数扩张，其中 $\mathfrak{S}$ 是一个不可約集合，从而 $\mathbf{P}(\mathfrak{S})$ 是 $\mathbf{P}$ 的一个純超越扩张．这也就是說，Ω 可由 $\mathbf{P}$ 先作一純超越扩张，然后再在这一基础之上作一純代数扩张得到．

通过上面几个定理作出的不可約集合 $\mathfrak{M}'$ 当然不是唯一的，可是它的势［因而純超越扩张 $\mathbf{P}(\mathfrak{M}')$ 的类型］却是唯一地确定的．事实上，下面的定理成立：

两个彼此等价的不可約集合 $\mathfrak{M}$ 和 $\mathfrak{N}$ 是等势的．

关于这一定理的一般証明，可参看 *Journal f. d. reine u. angew. Math.*, **137** 卷中 Steinitz 的原作或 O. Haupt，代数学引論 II，23 章 6 节．一个最重要的特殊情形，就是集合 $\mathfrak{M}$ 和 $\mathfrak{N}$ 当中至少有一个是有限集合的情况．事实上，設 $\mathfrak{M}$ 由 r 个元素 $u_1, u_2, \cdots, u_r$ 組成，那末根据 § 36 推論 4，$\mathfrak{N}$ 也不可能包含多于 r 个元素，因而 $\mathfrak{N}$ 也是有限的．另一方面，根据同样的理由，$\mathfrak{M}$ 也不可能

比 $\mathfrak{N}$ 包含更多的元素，因此 $\mathfrak{M}$ 和 $\mathfrak{N}$ 等势。

和 Ω 等价的不可約集合 $\mathfrak{M}'$ 的唯一地确定的势，称为域 Ω（对域 $\mathbf{P}$）的超越次数。

定理. 如果一个扩张可以依次作两个（有限）超越次数分别为 s 和 t 的扩张得到，那末这个扩张的超越次数等于 $s+t$[1]。

証明. 設 $\mathbf{P}\subseteq\Sigma\subseteq\Omega$. 設 $\mathfrak{S}$ 是 Σ 中一个对 $\mathbf{P}$ 来說不可約而与 Σ 等价的集合，$\mathfrak{T}$ 是 Ω 中一个对 Σ 来說不可約而与 Ω 等价的集合，那末 $\mathfrak{S}$ 的势是 s，而 $\mathfrak{T}$ 的势是 t，并且 $\mathfrak{S}$ 和 $\mathfrak{T}$ 沒有公共元素，因而 $\mathfrak{S}\vee\mathfrak{T}$ 的势是 $s+t$，如果我們能够証明 $\mathfrak{S}\vee\mathfrak{T}$ 对 $\mathbf{P}$ 不可約且与 Ω 等价，那末我們的証明就完成了。

Ω 对 $\Sigma(\mathfrak{T})$ 是代数的，Σ 对 $\mathbf{P}(\mathfrak{S})$ 是代数的。因此，Ω 对 $\mathbf{P}(\mathfrak{S},\mathfrak{T})$ 是代数的，即 Ω 和 $\mathfrak{S}\vee\mathfrak{T}$ 等价。

如果 $\mathfrak{S}\vee\mathfrak{T}$ 中某有限多个元素之間存在一个系数属于 $\mathbf{P}$ 的代数关系，那末首先可以断定，$\mathfrak{T}$ 中的元素事实上不可能出現在这个关系中。不然的話，在 $\mathfrak{T}$ 中的这样一些元素之間就会有一个系数属于 Σ 的代数关系，而这是和 $\mathfrak{T}$ 的不可約性相违背的。因此，$\mathfrak{S}$ 中的元素之間存在一个关系，而这又和 $\mathfrak{S}$ 的不可約性相矛盾。由此可知，$\mathfrak{S}\vee\mathfrak{T}$ 对 $\mathbf{P}$ 来說是不可約的。这就証明了定理。

§66. 代数函数的微分法

在 §23 中給出的多項式 $f(x)$ 的导数的定义，可以直接推广于系数属于域 $\mathbf{P}$ 的、一个不定元的有理函数

$$\varphi(x)=\frac{f(x)}{g(x)}.$$

1）这个定理对无限超越次数也成立，但是要用到无限势相加的概念，而这是我們所沒有講过的。

事实上，如果我們作差

$$\varphi(x+h)-\varphi(x)=\frac{f(x+h)g(x)-f(x)g(x+h)}{g(x)g(x+h)},$$

则当 $h=0$ 时这个分式的分子等于零。 因此分子中含有因子 h。两端同除以 h 即得

$$(1)\qquad \frac{\varphi(x+h)-\varphi(x)}{h}=\frac{q(x,h)}{g(x)g(x+h)}.$$

右端是 h 的一个有理函数，当 $h=0$ 时，由于分母不为零，故这个有理函数有完全确定的值。 这个值称为有理函数 $\varphi(x)$ 的**微商**或**导数** $\varphi'(x)$：

$$(2)\qquad \varphi'(x)=\frac{d\varphi(x)}{dx}=\frac{q(x,0)}{g(x)^2}.$$

为了实际計算 $q(x,0)$，我們把 (1) 中右端的分子按 h 的升冪展开，除以 h 再命 $h=0$，这样就得到

$$q(x,0)=f'(x)g(x)-f(x)g'(x),$$

以此式代入 (2) 即得商的微商的熟知的公式

$$\frac{d}{dx}\frac{f(x)}{g(x)}=\frac{f'(x)g(x)-f(x)g'(x)}{g(x)^2}.$$

設 $R(u_1,\cdots,u_n)$ 是一个有理函数，它对不定元 $u_1,\cdots,u_n$ 的偏导数是 $R'_1,\cdots,R'_n$。再設 $\varphi_1,\cdots,\varphi_n$ 是 x 的有理函数。

我們要証明**全微商公式**：

$$(3)\qquad \frac{d}{dx}R(\varphi_1,\cdots,\varphi_n)=\sum_1^n R'_\nu(\varphi_1,\cdots,\varphi_n)\frac{d\varphi_\nu}{dx}.$$

为了这个目的，我們根据微商的定义命

$$\varphi_\nu(x+h)-\varphi_\nu(x)=h\psi_\nu(x,h),\quad \psi_\nu(x,0)=\varphi'_\nu(x),$$

并命

$$
(4)\quad \begin{cases} R(u_1+h_1, \cdots, u_n+h_n) - R(u_1, \cdots, u_n) \\ = \sum_{\nu=1}^{n} \{R(u_1+h_1, \cdots, u_\nu+h_\nu, u_{\nu+1}, \cdots, u_n) - \\ \qquad - R(u_1+h_1, \cdots, u_\nu, u_{\nu+1}, \cdots, u_n)\} \\ = \sum_{\nu=1}^{n} h_\nu S_\nu(u_1+h_1, \cdots, u_\nu, h_\nu, u_{\nu+1}, \cdots, u_n); \end{cases}
$$

其中

$$S_\nu(u_1, \cdots, u_\nu, 0, u_{\nu+1}, \cdots, u_n) = R'_\nu(u_1, \cdots, u_n).$$

在恆等式(4)中命

$$u_\nu = \varphi_\nu(x), \quad h_\nu = \varphi_\nu(x+h) - \varphi_\nu(x) = h\psi_\nu(x, h),$$

并除以 h 則得

$$\frac{R(\varphi_1(x+h), \cdots, \varphi_n(x+h)) - R(\varphi_1(x), \cdots, \varphi_n(x))}{h}$$

$$= \sum_{\nu=1}^{n} \psi_\nu(x, h) S_\nu(\varphi_1 + h\psi_1, \cdots, \varphi_\nu, h\psi_\nu, \varphi_{\nu+1}, \cdots, \varphi_n)$$

現在在右端命 $h=0$，卽有

$$\frac{d}{dx} R(\varphi_1, \cdots, \varphi_n) = \sum \varphi'_\nu(x) R'_\nu(\varphi_1, \cdots, \varphi_n).$$

这就証明了(3)。

現在我們要把微分法的理論推广到一个变量 x 的代数函数去。所謂不定元 x 的一个代数函数，指的就是 $\mathbf{P}(x)$ 的一个代数扩张中的一个任意的元素 η。这里我們只作一个假定，卽 η 对 $\mathbf{P}(x)$ 是可分的。

这样，代数函数 η 就是 $\mathbf{P}(x)$ 上一个可分不可約多項式 $F(x, y)$ 的一个零点：

$$F(x, \eta) = 0.$$

$F(x, y)$ 对 x 和 y 的偏导数分别記作 F'_x 和 F'_y。由于可分性，$F'_y(x, y)$ 和 $F(x, y)$ 沒有公共零点。因此

$$F'_y(x, \eta) \neq 0.$$

在給出导数 $\frac{d\eta}{dx}$ 的一个合适的定义时，我們当然会期望全微商的規則对多項式 $F(x, y)$ 成立，即希望有

$$F'_x(x, \eta) + \frac{d\eta}{dx} F'_y(x, \eta) = 0.$$

因此我們**定义**

$$\frac{d\eta}{dx} = -\frac{F'_x(x, \eta)}{F'_y(x, \eta)}. \tag{5}$$

立即可以看出，这个定义实际上和定义多項式 $F(x, y)$ 的选择无关. 事实上，如果将 $F(x, y)$ 換成 $F(x, y)\cdot\psi(x)$，其中 $\psi(x)$ 为 x 的任意有理函数，則(5)中的 $F'_x(x, \eta)$ 和 $F'_y(x, \eta)$ 将被換成

$$F'_x(x, \eta)\cdot\psi(x) + F(x, \eta)\cdot\psi'(x) = F'_x(x, \eta)\psi(x)$$

和

$$F'_y(x, \eta)\cdot\psi(x),$$

而这是不会改变二者的商(5)的.

特別，如果 $\eta = c$ 是 $\mathbf{P}$ 中的常数，那末在 η 的定义方程中 x 根本不会出現，因此 $\frac{dc}{dx} = 0$.

現在設 ζ 是域 $\mathbf{P}(x, \eta)$ 中的一个元素，即 x 和 η 的一个有理函数，并且对 η 是有理整的：

$$\zeta = \varphi(x, \eta).$$

我們要对这个函数 φ 証明全微商規則：

$$\frac{d\zeta}{dx} = \varphi'_x(x, \eta) + \varphi'_y(x, \eta)\frac{d\eta}{dx}, \tag{6}$$

其中 φ'_x 和 φ'_y 代表 $\varphi(x, y)$ 对 x 和 y 的偏导数. 为了这个目的，我們作出 ζ 的定义方程：

$$G(x, \zeta) = 0,$$

并可設这个方程对 x 和 ζ 是有理整的。将 ζ 的表达式 $\varphi(x, \eta)$ 代到这个方程中去，并将 η 换成不定元 y。 这样得到的 y 的多項式以 η 为它的一个零点，因而可被 $F(x, y)$ 整除

$$G(x, \varphi(x, y)) = Q(x, y)F(x, y).$$

利用全微商規則 (3) 将这个恆等式分别对 x 和 y 微分之得

$$\begin{cases} G'_x(x, \varphi(x, y)) + G'_z(x, \varphi(x, y))\varphi'_x(x, y) = \\ \qquad\qquad = QF'_x + Q'_xF(x, y), \\ G'_z(x, \varphi(x, y))\varphi'_y(x, y) = QF'_y + Q'_yF(x, y). \end{cases}$$

再将 y 换成 η，这时含有 $F(x, y)$ 的項将成为零。其次，根据定义 (5)，命

$$F'_x(x, \eta) = -F'_y(x, \eta) \cdot \frac{d\eta}{dx},$$

$$G'_x(x, \zeta) = -G'_z(x, \zeta) \cdot \frac{d\zeta}{dx},$$

即得

$$\begin{cases} -G'_z(x, \zeta) \cdot \dfrac{d\zeta}{dx} + G'_z(x, \zeta)\varphi'_x(x, \eta) = \\ \qquad\qquad\qquad = -Q(x, \eta)F'_y(x, \eta) \cdot \dfrac{d\eta}{dx} \\ G'_z(x, \zeta)\varphi'_y(x, \eta) = Q(x, \eta)F'_y(x, \eta). \end{cases}$$

将第二个方程乘以 $\dfrac{d\eta}{dx}$ 加到第一个方程上去，并将整个式子除以 G'_z，即得

$$-\frac{d\zeta}{dx} + \varphi'_x(x, \eta) + \varphi'_y(x, \eta) \cdot \frac{d\eta}{dx} = 0,$$

这就証明了 (6)。

通过这样一些計算証明了特殊情形(6)之后，一般的**全微商規則**的証明就不再費力了。这个規則說：**如果** $\eta_1, \cdots, \eta_n$ **是一个域中** x **的可分代数函数**，而 $R(u_1, \cdots, u_n)$ **是一个多項式，其偏导数**

为 R'_ν，則

(7) $$\frac{d}{dx}R(\eta_1, \cdots, \eta_n) = \sum_1^n R'_\nu(\eta_1, \cdots, \eta_n)\frac{d\eta_\nu}{dx}.$$

証明。 設 ϑ 是 $\mathbf{P}(x)$ 的可分扩域 $\mathbf{P}(x, \eta_1, \cdots, \eta_n)$ 的一个本原元素，那末所有的 η_ν 都可以表成 x 和 ϑ 的有理函数：

$$\eta_\nu = \varphi_\nu(x, \vartheta).$$

如果 $\varphi'_{\nu x}$ 和 $\varphi'_{\nu t}$ 是 $\varphi_\nu(x, t)$ 对 x 和 t 的偏导数，則根据(6)有

$$\frac{d\eta_\nu}{dx} = \varphi'_{\nu x}(x, \vartheta) + \varphi'_{\nu t}(x, \vartheta)\cdot\frac{d\vartheta}{dx}.$$

同样，如果 R'_x 和 R'_t 是函数 $R(\varphi_1(x, t), \cdots, \varphi_n(x, t))$ 的偏导数，則

$$\frac{d}{dx}R(\eta_1, \cdots, \eta_n) = \frac{d}{dx}R(\varphi_1(x, \vartheta), \cdots, \varphi_n(x, \vartheta))$$

$$= R'_x(x, \vartheta) + R'_t(x, \vartheta)\cdot\frac{d\vartheta}{dx}.$$

但根据 (3) 我們有

$$R'_x(x, t) = \sum_1^n R'_\nu(\varphi_1(x, t), \cdots, \varphi_n(x, t))\varphi'_{\nu x}(x, t),$$

$$R'_t(x, t) = \sum_1^n R'_\nu(\varphi_1(x, t), \cdots, \varphi_n(x, t))\varphi'_{\nu t}(x, t),$$

故得

$$\frac{d}{dx}R(\eta_1, \cdots, \eta_n) = \sum_1^n R'_\nu(\varphi_1(x, \vartheta), \cdots, \varphi_n(x, \vartheta))\times$$

$$\times\left\{\varphi'_{\nu x}(x, \vartheta) + \varphi'_{\nu t}(x, \vartheta)\cdot\frac{d\vartheta}{dx}\right\}$$

$$= \sum_1^n R'_\nu(\eta_1, \cdots, \eta_n)\frac{d\eta_\nu}{dx}.$$

一般規則(7)的几个重要的特殊情形是：

$$\frac{d}{dx}(\eta+\zeta)=\frac{d\eta}{dx}+\frac{d\zeta}{dx}, \tag{8}$$

$$\frac{d}{dx}\eta\zeta=\eta\frac{d\zeta}{dx}+\zeta\frac{d\eta}{dx}, \tag{9}$$

$$\frac{d}{dx}\frac{\eta}{\zeta}=\frac{1}{\zeta^2}\left(\zeta\frac{d\eta}{dx}-\eta\frac{d\zeta}{dx}\right), \tag{10}$$

$$\frac{d}{dx}\eta^r=r\eta^{r-1}\frac{d\eta}{dx}. \tag{11}$$

显然，微商的定义(5)不仅当 x 为不定元时适用，当 x 是基域 $\mathbf{P}$ 上的超越元素，而 η 是 $\mathbf{P}(x)$ 上的可分代数元素时也是适用的。我們經常把 x 改写成 ξ. 由于这个原因，在 $\mathbf{P}$ 上一个超越次数为 1 的域中，我們可以对超越元素 ξ 求所有元素 η 的微商，只要后者对 $\mathbf{P}(\xi)$ 为可分就行.

設 η, ζ 和 ξ 代数相关，則域 $\mathbf{P}(\xi, \eta, \zeta)$ 对域 $\mathbf{P}$ 的超越次数为 1. 如果 η 对 $\mathbf{P}$ 是超越的，則 ζ 和 η 代数相关，因此我們可以作出微商 $\dfrac{d\zeta}{d\eta}$. 設

$$G(\eta, \zeta)=0 \tag{12}$$

是 ζ 在 $\mathbf{P}(\eta)$ 上的定义方程，而 G'_y 和 G'_z 是 $G(y, z)$ 的偏导数，則有

$$G'_y(\eta, \zeta)+G'_z(\eta, \zeta)\frac{d\zeta}{d\eta}=0. \tag{13}$$

另一方面，将(12)对 ξ 微分之，根据全微商規則有

$$G'_y(\eta, \zeta)\frac{d\eta}{d\xi}+G'_z(\eta, \zeta)\frac{d\zeta}{d\xi}=0. \tag{14}$$

将(13)乘以 $d\eta/d\xi$ 并从所得等式中减去(14)，即得**連鎖規則**：

$$\frac{d\zeta}{d\xi}=\frac{d\zeta}{d\eta}\frac{d\eta}{d\xi}. \tag{15}$$

特别，当 $\zeta = \xi$ 时由(15)可得

$$\frac{d\xi}{d\eta} \cdot \frac{d\eta}{d\xi} = 1. \tag{16}$$

这样一来，我們就用純代数的方式对一个变量的代数函数推导出了普通微分学中的全部规則。这里沒有利用到任何极限的考虑。

第九章 实 域

在代数数域的研究中，除去代数性質外还有某些非代数的性質：絕对值 $|a|$，实性，正性等也起作用．下面所举的例子指明，这些性質不能由代数运算 $+$ 与 $\cdot$ 唯一地定义．

設 w 是方程 $x^4=2$ 的一个实根，iw 是它的一个純虛根．同构

$$\Gamma(w)\cong\Gamma(iw)$$

保持所有的代数性質；但是这个同构把实数 w 变到純虛数 iw，把正数 $w^2=\sqrt{2}$ 变到負数 $(iw)^2=-\sqrt{2}$，而把絕对值 >1 的数 $1+\sqrt{2}$ 变到絕对值 <1 的数 $1-\sqrt{2}$．

在討論过程中将看到，这些非代数的性質还是与某些代数性質有联系，譬如在全体代数数的域中（也就是属于 Γ 的代数封閉的扩域中）可以用代数的性質刻划出一系列的（不是一个）子域，它們的每一个都与全体实代数数的域代数等价．在这样一些域中选定一个之后，它的元素这时可以称为“实的”，于是我們就可以代数地来定义絕对值以及正性等概念．

但是在进入这个代数理論之前，我們先介紹一下在分析中通常所用的实数与复数的引入方法，这并不是由于在邏輯上是必要的，而是由于在我們知道了什么是实数与复数之后，这个純代数理論所提出的問題可以有更清楚的了解，同时也能就此談一下极为重要的順序与基本叙列的概念．

§67. 有 序 域

在这一节，我們用公理的方法来討論第一个非代数的性質：正

性以及由它决定的順序.

一个域K称为有序的，如果对于它的元素定义了一个性質，叫做正的（>0），这个性質满足以下要求：

1. 对于K的每个元素a，关系

$$a=0,\quad a>0,\quad -a>0$$

中恰有一个成立.

2. 如果$a>0$且$b>0$，則$a+b>0$且$ab>0$.

如果$-a>0$，我們就說，a是負的.

如果在一有序域中我們按以下規定一般地来定义一大小关系

$$a>b,\quad \text{說成：}\quad a\text{大于}b$$

$$(\text{或者}\quad b<a,\quad \text{說成：}\quad b\text{小于}a)$$

$$\text{当}\quad a-b>0,$$

那么不难証明，它适合集合論的順序公理. 对于任意两个元素a, b，必有$a<b$或者$a=b$或者$a>b$. 由$a>b$与$b>c$推出$a-b>0$与$b-c>0$，因之$a-c=(a-b)+(b-c)>0$；从而$a>c$. 和§3中一样我們还有，由$a>b$推出$a+c>b+c$以及在$c>0$的情形$ac>bc$. 最后，当a与b是正的，由$a>b$推出$a^{-1}<b^{-1}$（反之亦然），因为

$$ab(b^{-1}-a^{-1})=a-b.$$

在有序域中，所謂元素a的絕对值$|a|$是指元素$a, -a$中非負的那一个，絕对值的計算适合規則

$$|ab|=|a|\cdot|b|,$$

$$|a+b|\leqslant|a|+|b|.$$

对于第一个，我們不难分四个可能的情形：

$$a\geqslant 0,\qquad b\geqslant 0;$$

$$a\geqslant 0,\qquad b<0;$$

$$a < 0, \qquad b \geqslant 0;$$

$$a < 0, \qquad b < 0$$

来验証. 至于第二条規則，在 $a \geqslant 0, b \geqslant 0$ 的情形，等号显然成立，因为两边都等于非負数 $a + b$，在 $a < 0, b < 0$ 的情形也一样. 这时两边都等于非負数 $-(a + b)$. 在四个情形中还剩下当中的两个情形；只要考虑其中的一个：$a \geqslant 0, b < 0$ 就够了. 在这个情形有

$$a + b < a < a - b = |a| + |b|,$$

$$-a - b \leqslant -b \leqslant a - b = |a| + |b|,$$

因而

$$|a + b| \leqslant |a| + |b|.$$

我們也有

$$a^2 = (-a)^2 = |a|^2 \geqslant 0,$$

等号只在 $a = 0$ 时成立. 由此进一步推出，平方和总是 $\geqslant 0$，并且只有在加項中每个全为零时才会 $= 0$.

特别地，单位元素 $1 = 1^2$ 总是正的，同样，每个和 $n \cdot 1 = 1 + 1 + \cdots + 1$ 是正的. 因之不可能有 $n \cdot 1 = 0$. 这就是說：*有序域的特征是零.*

引理. *如果环 $\mathfrak{R}$ 是有序的，$\mathbf{K}$ 是 $\mathfrak{R}$ 的商域，那么 $\mathbf{K}$ 可以按一种方法且仅有一种方法定义成有序域，使 $\mathfrak{R}$ 在其中仍保持原来的序.*

假設 $\mathbf{K}$ 已經按所要的方式定义成有序的. $\mathbf{K}$ 中任意一个元素都具有形式 $a = b/c$（b, c 在 $\mathfrak{R}$ 中且 $c \neq 0$）. 由

$$\frac{b}{c} > 0 \quad 或者 = 0 \quad 或者 < 0,$$

乘上 c^2 就分别得出

$$bc > 0 \quad 或者 = 0 \quad 或者 < 0.$$

因之 $\mathbf{K}$ 的可能的序是被 $\mathfrak{R}$ 的序唯一决定的．反过来不难看出，规定

$$\frac{b}{c} > 0 \quad 当 \quad bc > 0$$

的确定义 $\mathbf{K}$ 的一个序，而 $\mathfrak{R}$ 在其中保持原来的序．

特別地，有理数域 Γ 的序只能按一种方法定义，因为整数环 C 显然只能有自然顺序．因之 $m/n > 0$，当 $m \cdot n$ 是一自然数．

两个有序域称为**相似同构的**，如果在它們之間有一同构映射，它把正元素总是变到正元素．

一个域称为**阿基米德有序的**[1]，如果在給定的顺序之下，对于每个域中元素 a 都有一"自然数" n 使 $n > a$．这时，对于每个元素 a 也有一个数 $-n < a$ 以及对于每个正的 a 有分数 $1/n < a$．例如，有理数域 Γ 是阿基米德有序的．如果一个域是非阿基米德有序的，那么其中必有"无穷大"元素，它大于所有的有理数，也有"无穷小"元素，它比所有的正有理数小，但大于零．

关于非阿基米德有序域的文献

Artin, E. u. O. Schreier: Algebraische Konstruktion reeller Körper (实域的代数构造), *Abh. Math. Sem. Hamburg*, **5** (1926), 83—115.

Baer, R.: Über nichtarchimedisch geordnete Körper (关于非阿基米德有序域), Sitzungsber. Heidelb. Ak. 8. Abhandlung, 1927.

习題． 1．有理系数多項式 $f(t)$ 称为正的，如果其中出現的不定元最高方冪的系数是正的．証明，这样就在多項式环 $\Gamma[t]$ 中，从而在它的分式域 $\Gamma(t)$ 中定义了一个顺序，这个顺序是非阿基米德的（t 是"无穷大"）．

2．設

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n,$$

其中 a_i 属于一有序域 $\mathbf{K}$．設 $\mathbf{M}$ 是元素 1 与 $|a_1| + \cdots + |a_n|$ 中較大的一

1）在几何中"阿基米德公理"就是：任一由給定的 P 出发的給定綫段 PQ，沿 PR 的方向伸长若干倍之后总能超过任意給定的点 R．

个。証明：

$$f(s) > 0 \quad 对于 \quad s > \mathbf{M},$$
$$(-1)^n f(s) > 0 \quad 对于 \quad s < -\mathbf{M}.$$

由此可見，如果 $f(s)$ 在 $\mathbf{K}$ 中有零点，那么一定在区域 $-\mathbf{M} \leqslant s \leqslant \mathbf{M}$ 中．

3．仍設 $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$，所有的 $a_i \geqslant -c$，$c \geqslant 0$． 証明：$f(s) > 0$ 对于 $s \geqslant 1 + c$． [利用不等式 $s^m > c(s^{m-1} + s^{m-2} + \cdots + 1)$．] 用 $-x$ 代 x，同样地求一个界 $-1 - c'$ 使 $(-1)^n f(s) > 0$ 当 $s < -1 - c'$． 如果除首項系数 1 以外，系数 $a_1, \cdots, a_r$ 也是正的，那么界 $1 + c$ 可以換成 $1 + \dfrac{c}{1 + a_1 + \cdots + a_r}$．

§68. 实数的定义

設 $\mathbf{K}$ 是一有序域，$\mathfrak{M}$ 是 $\mathbf{K}$ 中元素的一个非空集合． 如果 $\mathfrak{M}$ 的元素全小于或等于 $\mathbf{K}$ 中某一固定的元素 s，則 s 称为 $\mathfrak{M}$ 的一个**上界**，而 $\mathfrak{M}$ 称为**有上界的**． 如果有最小的上界，它就称为集合 $\mathfrak{M}$ 的**上限**． 同样定义下界与下限的概念．

在有理数域 Γ 中，并不是每个有上界的集合都有上限． 例：$\mathfrak{M}$ 是所有平方小于 3 的正数的集合． 每个平方大于 3 的正数都是 $\mathfrak{M}$ 的上界． 在 Γ 中沒有平方等于 3 的数，因为 $x^2 - 3$ 在 Γ 中是不可約的． 如果 r 是一正有理数，$r^2 > 3$，那么总有一个較小的正有理数，它的平方仍 > 3． 这就是說，对于每个 Γ 中的上界都有一更小的上界，因而上限不存在．

我們現在要来証明，对于每个有序域 $\mathbf{K}$ 都能找到一个有序扩域 Ω，在其中每个有上界的非空集合都有上限． 如果 $\mathbf{K}$ 特别就是有理数域，那么 Ω 将是熟知的"实数"域． 在各种分析基础中所熟悉的域 Ω 的构造法中，我們这里采取 Cantor 的用"基本叙列"的构造法．

由有序域 $\mathbf{K}$ 的元素 $a_1, a_2, \cdots$ 組成的无穷叙列称为一**基本叙**

列 $\{a_\nu\}$，如果对于 $\mathbf{K}$ 中每个正的 ε 都有一自然数 $n = n(\varepsilon)$ 使得

$$(1) \qquad |a_p - a_q| < \varepsilon \quad 对于 \quad p > n, q > n.$$

令 $q = n + 1$，由 (1) 推出

$$|a_p| \leqslant |a_q| + |a_p - a_q| < |a_{n+1}| + \varepsilon = \mathbf{M} 对 p > n.$$

因之每个基本叙列都是有上界和下界的。

基本叙列的和与积定义为

$$c_n = a_n + b_n; \quad d_n = a_n b_n.$$

和与积还是基本叙列，証明如下：对每个 ε 有 n_1 使

$$|a_p - a_q| < \frac{1}{2}\varepsilon \quad 对于 \quad p > n_1, q > n_1,$$

又有 n_2 使

$$|b_p - b_q| < \frac{1}{2}\varepsilon \quad 对于 \quad p > n_2, q > n_2.$$

如果 n 是 n_1 与 n_2 中較大的一个，則

$$|(a_p + b_p) - (a_q + b_q)| < \varepsilon \quad 对于 \quad p > n, q > n.$$

同样地，有 $\mathbf{M}_1$ 与 $\mathbf{M}_2$ 使

$$|a_p| < \mathbf{M}_1 \quad 对于 \quad p > n_1,$$

$$|b_p| < \mathbf{M}_2 \quad 对于 \quad p > n_2,$$

并且对每个 ε 有 $n' \geqslant n_2$ 与 $n'' \geqslant n_1$ 使

$$|a_p - a_q| < \frac{\varepsilon}{2\mathbf{M}_2} \quad 对于 \quad p > n', q > n',$$

$$|b_p - b_q| < \frac{\varepsilon}{2\mathbf{M}_1} \quad 对于 \quad p > n'', q > n''.$$

分别乘以 $|b_p|$ 与 $|a_q|$ 即得

$$|a_p b_p - a_q b_p| < \frac{\varepsilon}{2} \quad 对于 \quad p > n', q > n',$$

$$|a_q b_p - a_q b_q| < \frac{\varepsilon}{2} \quad 对于 \quad p > n'', q > n'',$$

因此，如果 n 是 n' 与 n'' 中較大的一个，則有

$$|a_p b_p - a_q b_q| < \varepsilon \quad 对于 \quad p > n,\ q > n.$$

基本叙列的加法与乘法显然适合环的全部公理；因之，基本叙列組成一个环 $\mathfrak{o}$.

"收斂于零"的基本叙列 $\{a_\nu\}$，也就是对每个 ε 都有 n 使

$$|a_p| < \varepsilon \quad 对于 \quad p > n,$$

称为一个零叙列. 我們現在証明：

零叙列在环 $\mathfrak{o}$ 中組成一个理想 $\mathfrak{n}$.

証明. 如果 $\{a_p\}$ 与 $\{b_p\}$ 是零叙列，那么对于每个 ε 有 n_1 与 n_2 使

$$|a_p| < \frac{1}{2}\varepsilon \quad 对于 \quad p > n_1,$$

$$|b_p| < \frac{1}{2}\varepsilon \quad 对于 \quad p > n_2,$$

因之，当 n 是 n_1 与 n_2 中較大的一个，則有

$$|a_p - b_p| < \varepsilon \quad 对于 \quad p > n;$$

从而 $\{a_p - b_p\}$ 也是零叙列. 又如果 $\{a_p\}$ 是一零叙列，$\{c_p\}$ 是任意一个基本叙列，那么我們决定 n' 与 $\mathbf{M}$ 使

$$|c_p| < \mathbf{M} \quad 对于 \quad p > n',$$

并且对每个 ε 决定 $n = n(\varepsilon) \geq n'$，使

$$|a_p| < \frac{\varepsilon}{\mathbf{M}} \quad 对于 \quad p > n.$$

由此推出

$$|a_p c_p| < \varepsilon \quad 对于 \quad p > n;$$

从而 $\{a_p c_p\}$ 也是零叙列.

同余类环 $\mathfrak{o}/\mathfrak{n}$ 称为 Ω. 我們来証明，Ω 是一域，这就是説，在 $\mathfrak{o}$ 中間余式

$$(2) \qquad ax \equiv 1(\mathfrak{n})$$

对于 $a \not\equiv 0(\mathfrak{n})$ 有解. 这里 1 表示 $\mathfrak{o}$ 的单位元素，也就是基本叙列 $\{1, 1, \cdots\}$.

一定有一个 n 与一个 $\eta > 0$ 使

$$|a_q| \geqslant \eta \quad 对于 \quad q > n.$$

因为假如对于所有的 n 与所有的 $\eta > 0$ 都有一个 $q > n$ 使

$$|a_q| < \eta,$$

那么对于給定的 η 我們总可以选择足够大的 n 使得，对于 $p > n$, $q > n$ 有

$$|a_p - a_q| < \eta.$$

由此推出，对所有的 $p > n$ 有

$$|a_p| < 2\eta,$$

这就是說，叙列 $\{a_p\}$ 是一零叙列，与假設矛盾。

如果我們把基本叙列 $\{a_p\}$ 中 $a_1, \cdots, a_n$ 換成 η，那么所得的叙列仍在同一个模 $\mathfrak{n}$ 的同余类中。仍用 $a_1, \cdots, a_n$ 来表示这 n 个新的元素 η，于是对**所有的** p 就有

$$|a_p| \geqslant \eta, \quad 特别地 \quad a_p \neq 0.$$

現在 $\{a_p^{-1}\}$ 是一基本叙列. 因为对每个 ε 都有一个 n 使

$$|a_q - a_p| < \varepsilon\eta^2 \quad 对于 \quad p > n, q > n.$$

假如对于一个 $p > n$ 与一个 $q > n$ 有 $|a_p^{-1} - a_q^{-1}| \geqslant \varepsilon$，那么乘上 $|a_p| \geqslant \eta$ 与 $|a_q| \geqslant \eta$ 即得

$$|a_q - a_p| = |a_p a_q(a_p^{-1} - a_q^{-1})| \geqslant \varepsilon\eta^2,$$

这是不可能的. 因之有

$$|a_p^{-1} - a_q^{-1}| < \varepsilon \quad 对于 \quad p > n, q > n.$$

基本叙列 $\{a_p^{-1}\}$ 显然就是同余式(2)的解.

域 Ω 特别地包含那些由形式为

$$\{a, a, a, \cdots\}$$

的基本叙列所代表的模 $\mathfrak{n}$ 的同余类. 它們組成一个与 $\mathbf{K}$ 同构的 Ω 的子环 $\mathbf{K}'$; 因为 $\mathbf{K}$ 中每个元素 a 都对应于一个这样的同余类, 不同的 a 对应于不同的同余类,并且和对应于和,积对应于积. 如果我們現在把 $\mathbf{K}'$ 的元素与 $\mathbf{K}$ 的元素等同起来, 那么 Ω 就是 $\mathbf{K}$ 的一个扩域.

基本叙列 $\{a_p\}$ 称为**正的**,如果在 $\mathbf{K}$ 中有一 $\varepsilon > 0$ 同时有一个 n 使

$$a_p > \varepsilon \quad 对于 \quad p > n.$$

两个正的基本叙列的和与积显然还是正的. 一个正的叙列 $\{a_p\}$ 与一个零叙列 $\{b_p\}$ 的和也一定是正的; 这一点可以証明如下, 选一足够大的 n 使

$$a_p > \varepsilon \quad 对于 \quad p > n,$$

$$|b_p| < \frac{1}{2}\varepsilon \quad 对于 \quad p > n,$$

由此即得 $a_p + b_p > \frac{1}{2}\varepsilon$ 对于 $p > n$. 因而在一模 $\mathfrak{n}$ 的同余类中只要有一个叙列是正的,所有的都是正的. 在这个情形,这个同余类本身就称为**正的**. 同余类 k 称为**負的**,如果 $-k$ 是正的.

如果 $\{a_p\}$ 与 $\{-a_p\}$ 都不是正的, 那么对每个 $\varepsilon > 0$ 与每个 n 有一 $r > n$ 与一 $s > n$ 使

$$a_r \leqslant \varepsilon \quad 与 \quad -a_s \leqslant \varepsilon.$$

选取足够大的 n 使得,对于 $p > n$, $q > n$ 有

$$|a_p - a_q| < \varepsilon,$$

首先取 $q = r$ 而 p 为任意 $> n$ 的数就有

$$a_p = (a_p - a_q) + a_r < \varepsilon + \varepsilon = 2\varepsilon,$$

再取 $q = s$ 而 p 为任意 $> n$ 的数就有

$$-a_p=(a_q-a_p)-a_s<\varepsilon+\varepsilon=2\varepsilon,$$

从而

$$|a_p|<2\varepsilon \quad 对于 \quad p>n.$$

因之 $\{a_p\}$ 是一零叙列.

以上討論說明,或者 $\{a_p\}$ 是正的或者 $\{-a_p\}$ 是正的或者 $\{a_p\}$ 是一零叙列，三者必居其一．因而模 n 的每个同余类是正的或者負的或者是零．因为正的同余类的和与积还是正的,所以得出結論：

Ω 是一有序域.

我們立即看出，**K** 在 Ω 中仍保持原来的順序.

如果叙列 $\{a_p\}$ 定义元素 α，叙列 $\{b_p\}$ 定义元素 β,那么由

$$a_p \geqslant b_p \quad 对于 \quad p>n$$

即得 $\alpha \geqslant \beta$．否則，設 $\alpha<\beta$，即 $\beta-\alpha>0$，于是对于基本叙列 $\{b_p-a_p\}$ 就有一个 ε 与一个 m 使

$$b_p-a_p>\varepsilon>0 \quad 对于 \quad p>m.$$

在这里取 $p=m+n$，就与假設 $a_p \geqslant b_p$ 矛盾．但是值得注意，由 $a_p>b_p$ 并不是推出 $\alpha>\beta$，而是推出 $\alpha \geqslant \beta$.

由于每个基本叙列都是有上界的，所以对于 Ω 中每个元素 ω 都有 **K** 中一个元素 s 比它大．如果 **K** 是阿基米德有序的，那么对于 s 又有一个比它大的自然数 n；从而对于每个 ω 也就有一个 $n>\omega$，这就是說，Ω 是阿基米德有序的.

在域 Ω 中我們自然又可以定义絕对值，基本叙列与零叙列的概念．零叙列也組成一个理想．如果叙列 $\{\alpha_p\}$ 模这个理想同余于一个常叙列 $\{\alpha\}$，即 $\{\alpha_p-\alpha\}$ 是一零叙列，那么我們就說，叙列 $\{\alpha_p\}$ 收斂于极限 α，記为

$$\lim_{p\to\infty}\alpha_p=\alpha \quad 或簡单地 \quad \lim\alpha_p=\alpha.$$

$\mathbf{K}$ 中的基本叙列 $\{a_p\}$ 一方面根据定义就代表 Ω 的元素，另一方面它也可以看成 Ω 的基本叙列，因为 $\mathbf{K}$ 包含在 Ω 中．我們現在証明：如果叙列 $\{a_p\}$ 定义 Ω 中元素 α，則 $\lim a_p = \alpha$．首先我們看到，对于 Ω 中每个正的 ε 一定有 $\mathbf{K}$ 的一个正元素 ε' 比它小，而对于 ε' 有一个 n 使得，对于 $p > n$, $q > n$ 必有

$$|a_p - a_q| < \varepsilon',$$

这就是説，$a_p - a_q$ 与 $a_q - a_p$ 都比 ε' 小．根据上面所作的説明，由此推出 $a_p - \alpha$ 与 $\alpha - a_p$ 都 $\leqslant \varepsilon'$，因而

$$|a_p - \alpha| \leqslant \varepsilon' < \varepsilon.$$

于是 $\{a_p - \alpha\}$ 是一零叙列．

我們現在来証明，通过基本叙列域 Ω 不可能再扩大，每个基本叙列 $\{\alpha_p\}$ 在 Ω 中已經有极限了（Cauchy 的收斂定理）．

証明中我們不妨假定，在叙列 $\{\alpha_p\}$ 中相邻的两个元素 α_p, α_{p+1} 总是不同的．假如不是这样，我們或者可以选出一个子叙列，它由那些与 α_{p-1} 不同的 α_p 組成，于是由子叙列的收斂性立即推出整个叙列的收斂性，或者就是叙列 $\{\alpha_p\}$ 由某一个位置开始是常量：$\alpha_p = \alpha$ 当 $p > n$；这时，自然有 $\lim \alpha_p = \alpha$．

設

$$|\alpha_p - \alpha_{p+1}| = \varepsilon_p.$$

因为 $\{\alpha_p\}$ 是一基本叙列，所以 $\{\varepsilon_p\}$ 是一零叙列[1]．根据假定，$\varepsilon_p > 0$．

对于每个 α_p 我們現在选取一个近似元素 a_p，它具有性質

$$|a_p - \alpha_p| < \varepsilon_p.$$

1）証明的前一部分只是为了肯定地給出一个零叙列，它在下面要用到．在阿基米德的情形，我們就可以簡单地取 $\varepsilon_p = 2^{-p}$；但是我們希望在一般的假定下来証明这个定理．在非阿基米德的情形，$\{2^{-p}\}$ 不是零叙列．

这是可能的，因为 α_p 本身就是由一个以 α_p 为极限的基本叙列 $\{a_{p1}, a_{p2}, \cdots\}$ 所定义。对于每个 ε 都有一个 n' 使

$$|\alpha_p - \alpha_q| < \frac{1}{3}\varepsilon \quad 对于 \quad p > n', q > n'$$

以及有一个 n'' 使

$$\varepsilon_p < \frac{1}{3}\varepsilon \quad 对于 \quad p > n''.$$

如果 n 是数 n' 与 n'' 中較大的一个，那么对于 $p > n$, $q > n$, 三个絕对值 $|a_p - \alpha_p|$, $|\alpha_p - \alpha_q|$ 与 $|\alpha_q - a_q|$ 全小于 $\frac{1}{3}\varepsilon$, 因之

$$\begin{aligned}|a_p - a_q| &\leqslant |a_p - \alpha_p| + |\alpha_p - \alpha_q| + |\alpha_q - a_q| \\ &< \frac{1}{3}\varepsilon + \frac{1}{3}\varepsilon + \frac{1}{3}\varepsilon = \varepsilon.\end{aligned}$$

于是 a_p 組成 $\mathbf{K}$ 中的一个基本叙列，它定义 Ω 的一个元素 ω. 叙列 $\{\alpha_p\}$ 与这个基本叙列只相差一个零叙列 $\{a_p - \alpha_p\}$，因而它們有相同的极限 ω.

我們現在要来对于 $\mathbf{K}$ 是阿基米德有序的，因而 Ω 也是阿基米德有序的情形，証明关于上限的定理：

在 Ω 中每个有上界的非空集合 $\mathfrak{M} \subset \Omega$ 都有上限.

証明. 設 s 是 $\mathfrak{M}$ 的一个上界，M 是一个 $> s$ 的整数(当然也是一个上界)，μ 是 $\mathfrak{M}$ 中任意一个元素而 m 是一个 $> -\mu$ 的整数. 于是

$$-m < \mu < M.$$

对于每个自然数 p 我們来作有限多个"在 $-m$ 与 M 之間"的分数 $k \cdot 2^{-p}$(k 是整数)：

$$-m \leqslant k \cdot 2^{-p} \leqslant M.$$

在这些分数中我們来找一个最小的，但它还是 $\mathfrak{M}$ 的上界. 这样的

分数是存在的，因为M本身就是一个。

用a_p表示这个最小的上界。于是a_p-2^{-p}就不再是上界，因而对于每个$q>p$有

(3) $$a_p-2^{-p}<a_q\leqslant a_p.$$

由此推出

$$|a_p-a_q|<2^{-p},$$

从而

(4) $$|a_p-a_q|<2^{-n} \quad 对于 \quad p>n, q>n.$$

对于任給的ε我們总能找到一个自然数$h>\varepsilon^{-1}$以及一个$2^n>h>\varepsilon^{-1}$。于是有$2^{-n}<\varepsilon$。因之(4)說明了，$\{a_p\}$是一个基本叙列，它就定义了Ω中一个元素ω。由(3)还推出

$$a_p-2^{-p}\leqslant\omega\leqslant a_p.$$

ω是$\mathfrak{M}$的一个上界；这就是說，$\mathfrak{M}$的所有元素μ都$\leqslant\omega$。假如有一个$\mu>\omega$，那么就可以找到一个数$2^p>(\mu-\omega)^{-1}$；于是有$2^{-p}<\mu-\omega$。把上面的不等式与$a_p-2^{-p}\leqslant\omega$相加，卽得$a_p<\mu$，这是不可能的，因为$a_p$是$\mathfrak{M}$的一个上界。

ω是$\mathfrak{M}$的最小上界。假如σ比它更小，那么就可以找到一个数p使$2^{-p}<\omega-\sigma$。因为a_p-2^{-p}不是$\mathfrak{M}$的上界，所以$\mathfrak{M}$中有一个μ使$a_p-2^{-p}<\mu$。由此推出

$$a_p-2^{-p}<\sigma,$$

再与上面的不等式相加卽得

$$a_p<\omega,$$

这是不可能的。因之ω是$\mathfrak{M}$的上限。

以上的构造法对于每个有序域$\mathbf{K}$給出一个唯一决定的有序扩域Ω，当$\mathbf{K}$是阿基米德有序时，关于上限的定理在Ω中成立。如果$\mathbf{K}$特别是有理数域，那么Ω就是实数域。因之在这个理論

中，实数就是有理数的基本叙列环中模 n 的一个同余类。

习题. 1. 証明极限概念的下列性质：

a) 如果 $\{\alpha_n\}$ 与 $\{\beta_n\}$ 是收敛的叙列，则

$$\lim(\alpha_n \pm \beta_n) = \lim \alpha_n \pm \lim \beta_n,$$
$$\lim \alpha_n\beta_n = \lim \alpha_n \cdot \lim \beta_n.$$

b) 如果 $\lim \beta_n \neq 0$ 并且所有的 $\beta_n \neq 0$，则

$$\lim(\beta_n^{-1}) = (\lim \beta_n)^{-1}.$$

c) 收敛叙列的子叙列还是收敛的并有相同的极限。

2. 每个阿基米德有序域都相似同构于实数域的一个子域。［域中每个元素 β 都可以表示成一个有理数基本叙列的极限，这个基本叙列同时也定义一个实数 β'，$\beta\to\beta'$ 就是一个同构。］

3. 每个实数 s 都可以表成无穷小数

$$s = a_0 + \sum_{\nu=1}^{\infty} a_\nu 10^{-\nu}\left(\text{这就是 } s = \lim_{n\to\infty}\left(a_0 + \sum_{\nu=1}^{n} a_\nu 10^{-\nu}\right)\right)$$
$$(0 \leqslant a_\nu < 10).$$

§69. 实函数的零点

設 $\mathbf{P}$ 是实数域。我們現在来考虑实变数 x 的实值函数 $f(x)$。这样一个函数称为在 $x = a$ 处連續，如果对于每个 $\epsilon > 0$ 都有 $\delta > 0$ 使得

$$|f(a + h) - f(a)| < \epsilon \quad \text{对于} \quad |h| < \delta.$$

容易証明，連續函数的和与积还是連續函数（参考 §68 中对于基本叙列相应的証明）。因为常量与函数 $f(x) = x$ 是到处連續的函数，所以所有的 x 的多項式都表示到处連續的函数。

Weierstrass 的关于連續函数的零点定理是：

$f(x)$ 是在 $a\leqslant x\leqslant b$ 上的連續函数，如果 $f(a) < 0$ 与 $f(b) > 0$，则 $f(x)$ 在 a 与 b 之間有一零点。

証明. 設 c 是 a 与 b 之間所有使 $f(x) < 0$ 的 x 的上限。于

是有三个可能性：

1. $f(c)>0$. 这时一定是 $c>a$ 并且有一 $\delta>0$ 使得，对于 $0<h<\delta$

$$|f(c-h)-f(c)|<f(c),$$
$$f(c)-f(c-h)<f(c),$$

这就是說

$$f(c-h)>0,$$
$$f(x)>0 \quad 对于 \quad c-\delta<x\leqslant c.$$

因之 $c-\delta$ 是使 $f(x)<0$ 的 x 的一个上界. 但 c 已經是最小上界，所以这个情形不可能.

2. $f(c)<0$. 这时必有 $c<b$ 并且有一 $\delta>0$ 使得，对于 $0<h<\delta$, 譬如說，$h=\frac{1}{2}\delta$

$$f(c+h)-f(c)<-f(c),$$
$$f(c+h)<0.$$

于是 c 就不是使 $f(x)<0$ 的 x 的上界了. 因之这个情形也不可能.

3. $f(c)=0$ 是仅有剩下的情形，所以 $f(x)$ 有零点 c.

Weierstrass 的关于多項式的零点定理是所有关于代数方程的实根的定理的基础. 以后我們将要把它推广到实数域以外的某些域上，即推广到所謂"实封闭域"上. 这一节中以后的定理全部只依赖于关于多項式的 Weierstrass 零点定理，因而它們对于以后更一般的域也成立.

推論. 1. 对于 $d>0$ 与每个自然数 n，多項式 x^n-d 一定有一个正实根.

因为对 $x=0$ 有 $x^n-d<0$，而对于大的 $x\left(例如, x>1+\frac{d}{n}\right)$

有 $x^n - d > 0$.

由 $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$ 进一步推知，当 $a > b > 0$ 时有 $a^n > b^n$，因而方程 $x^n = d$ 只能有一个正实根. 这个根用 $\sqrt[n]{d}$ 表示，当 $n = 2$，簡記为 $\sqrt{d}$（"平方根"）. 令 $\sqrt[n]{0} = 0$. 由 $a > b \geqslant 0$ 也推出 $\sqrt[n]{a} > \sqrt[n]{b}$，否則，假如 $\sqrt[n]{a} \leqslant \sqrt[n]{b}$，就要推出 $a \leqslant b$ 了.

2. 每个奇次多項式在 **P** 中有一个零点.

因为根据 § 67 的习題 2，有一个 **M** 使得 $f(\mathbf{M}) > 0$ 而 $f(-\mathbf{M}) < 0$.

我們現在来討論一个多項式 $f(x)$ 的实根的計算間題. 按实数的定义，所謂計算就是求任意与之逼近的有理数.

在 § 67（习題 2）中我們已經看到，如何求 $f(x)$ 实根的界：如果

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n,$$

而 **M** 是 1 与 $|a_1| + \cdots + |a_n|$ 中較大的一个，那么 $f(x)$ 所有的根全在 $-\mathbf{M}$ 与 **M** 之間. **M** 可以用一个（較大的）有理数代替，还称为 **M**，然后我們把区間 $-\mathbf{M} \leqslant x \leqslant \mathbf{M}$ 用有理的中間点分成任意小的部分. 如果我們有一个方法来判断，在两个給定的界限之間究竟有多少个根，那么就能断定根在那几部分之中. 把根所在的区間再进一步分割，我們就能得到实根的任意近似的值.

一个判别在两个給定的界限之間有多少个根或者是全部有多少个根的方法是

Sturm 定理. 对于一給定的多項式 $X = f(x)$ 按下面的办法决定多項式 $X_1, X_2, \cdots, X_r$:

$$X_1 = f'(x) \quad （求微商）$$

$$
(1) \qquad \left\{
\begin{array}{l}
X \;\,= Q_1X_1 - X_2, \\
X_1 = Q_2X_2 - X_3, \\
\cdots\cdots\cdots\cdots\cdots \\
X_{r-1} = Q_rX_r
\end{array}
\right\} \quad \text{(輾轉相除法)}.
$$

对于每个不是 $f(x)$ 的零点的实数 a,設 $w(a)$ 是数列

$$X(a),\ X_1(a),\ \cdots,\ X_r(a)$$

的变号数[1]. 如果 b 与 c 是任意的数, $b<c$ 并且都不使 $f(x)$ 为零,那在区間 $b\leqslant x\leqslant c$ 中不同的零点的个数(重根只数一次!)等于

$$w(b)-w(c).$$

多項式敘列 $X,\ X_1,\ \cdots,\ X_r$ 称为 $f(x)$ 的 Sturm 組. 定理就是說,在 b 与 c 之間零点的个数等于由 b 变到 c 时 Sturm 組的变号数的差額.

証明. 最后一个多項式 X_r 显然就是 $X=f(x)$ 与 $X_1=f'(x)$ 的最大公因子. 如果把 Sturm 組中的多項式全用 X_r 除一下,那么 $f(x)$ 就不再有重的綫性因子,而对于非零点的 a 并不影响变号数;因为除了以后, Sturm 組中每一項的符号或者全不变或者全反个号. 因之在証明中我們不妨假定 Sturm 組的最后一項是一个非零常数. 这时, Sturm 組的第二項就不再是第一項的微商:譬如 d 是 $f(x)$ 的 l 重零点,即

$$X=f(x)=(x-d)^l g(x),\ g(d)\neq 0,$$

$$X_1=f'(x)=l(x-d)^{l-1}g(x)+(x-d)^l g'(x),$$

于是消去因子 $(x-d)^{l-1}$ 之后即得

---

1) 所謂一个数 c 的符号是指+,-或者 0,就看 c 是正的,还是負的或者 0.在一个仅由符号+与-組成的敘列中,一个+緊接着一个-或者一个-緊接着一个+称为一个变号.如果还有 0 出現,在計算变号时就簡单地把它略去.

$$\bar{X} = (x - d)g(x),$$
$$\bar{X}_1 = l \cdot g(x) + (x - d)g'(x),$$

对于其它的根 d', d'', …就再去掉一些公因子. 修改过的 Sturm 組的多項式仍用 $X = X_0, X_1, \cdots, X_r$ 表示.

在这个假定下, Sturm 組中相邻的两項不可能有公根. 否則, 設 $X_k(a)$ 与 $X_{k+1}(a)$ 同时等于零, 于是由方程 (1) 就可以推知, $X_{k+1}(a), \cdots, X_r(a)$ 也都为零, 但 $X_r =$ 常数 $\neq 0$.

Sturm 組中多项式的零点把区間 $b \leqslant x \leqslant c$ 分成一些子区間. 在每个这样的子区間中, X 以及每个 X_r 全不为零, 根据 Weierstrass 零点定理可知, 在每个这样的区間之內 Sturm 組中多項式全不变号, 因而数 $w(a)$ 也保持不变. 因之我們只需要考察数 $w(a)$ 在 Sturm 組的某一个多項的零点 d 处如何改变.

首先設 d 是 $X_k(0 < k < r)$ 的一个零点. 根据方程

$$X_{k-1} = Q_k X_k - X_{k+1},$$

数 $X_{k-1}(d)$ 与 $X_{k+1}(d)$ 必反号. 因之 X_{k-1} 与 X_{k+1} 在以 d 为端点的两个子区間上也反号. 現在不論 X_k 有什么符号 (+, − 或者 0), X_{k-1} 与 X_{k+1} 之間的变号数总是一样的: 一定是一次变号. 因之經过点 d 时数 $w(a)$ 根本不改变.

再設 d 是 $f(x)$ 的零点, 按开始处作的説明, 譬如

$$X = (x - d)g(x), \quad g(d) \neq 0,$$
$$X_1 = l \cdot g(x) + (x - d)g'(x),$$

这里 l 是一自然数. X_1 在点 d 处, 因而在以 d 为端点的两个子区間上的符号都等于 $g(d)$ 的符号, 而 X 在这些点的符号就是 $(x - d)g(d)$ 的符号. 因之对于 $a < d$, 在 $X(a)$ 与 $X_1(a)$ 之間有一个变号, 而对于 $a > d$ 就不再有变号. Sturm 組中其余的变号在經过点 d 时保持不变, 这一点上面已經証明. 因之在經过点 d 时,

数 $w(a)$ 減少 1. 这就証明了 Sturm 定理.

如果我們要利用 Sturm 定理来决定 $f(x)$ 不同的实根的总数，那么必須取下界 b 与上界 c 使 $f(x)$ 在 $x < b$ 处与 $x > c$ 处不再有根. 譬如說，就可以选 $b = -\mathbf{M}$ 与 $c = \mathbf{M}$. 更簡单一些是选取 b 与 c 使 Sturm 組中多項式在 $x < b$ 与 $x > c$ 处全沒有根. 这样，Sturm 組中多項式的符号就可以由它們首項系数的符号决定: $a_0x^m + a_1x^{m-1} + \cdots$ 对于非常大的 x 与 a_0 同号，对于非常小的(負的) x 与 $(-1)^m a_0$ 同号. 至于 b 与 c 究竟需要多大的問題在这里是无需解决的: 我們只要把 Sturm 組中多項式的首項系数 a_0 与次数 m 算出来就行了.

习题. 1. 决定多項式

$$x^3 - 5x^2 + 8x - 8$$

实根的个数. 这些根在哪些相邻的整数之間?

2. 如果 Sturm 組中最后两个多項式 X_{r-1}, X_r 的次数是 1, 0, 那么常数 X_r (或者是它的符号，只是符号是有关系的)也可以这样来算出，即把 X_{r-1} 的零点代入 $-X_{r-2}$.

3. 如果在計算 Sturm 組的过程中出現一个 X_k, 它的符号根本不变(譬如說是平方和)，那么 Sturm 組就可以算到这里为止. 我們也可以从某一个 X_k 中消去一个恆正的因子，然后由这个修改过的 X_k 再往下算.

4. 在 Sturm 定理的証明中用到的多項式 X_1 [$f'(x)$ 的一个因子]在 $f(x)$ 两个相邻的根之間一定变号. 証明? 因之在 $f(x)$ 两个根之間 $f'(x)$ 至少有一个根 (Rolle 定理).

5. 由 Rolle 定理推导微分的中值定理，即是說，对于 $a < b$, 一定有一适当的 c, $a < c < b$ 使

$$\frac{f(b) - f(a)}{b - a} = f'(c).$$

[令

$$f(x) - f(a) - \frac{f(b) - f(a)}{b - a}(x - a) = \varphi(x).]$$

6. 如果在区間 $a \leqslant x \leqslant b$ 中有 $f'(x) > 0$, 則 $f(x)$ 是上升函数; 同样，如果 $f'(x) < 0$, 則 $f(x)$ 是下降函数.

7. 多項式 $f(x)$ 在每个区間 $a \leqslant x \leqslant b$ 中有最大値与最小値，它們或者在 $f'(x)$ 的零点处或者在端点 a, b 处达到.

§70. 复数域

如果我們在实数域 $\mathbf{P}$ 上添加在 $\mathbf{P}$ 中不可約多項式 x^2+1 的一个根 i，我們就得到复数域 $\Omega = \mathbf{P}(i)$.

以下所談到的"数"总是指复数(其中特别也包含实数). 代数数是指那些对于有理数域 Γ 是代数的数. 这样，所謂代数数域，实的数域等等的含意就清楚了. 按 § 38 中定理，所有的代数数組成一个域 $\mathbf{A}$，它包含所有的代数数域.

我們現在来証明：

在复数域中，方程 $x^2 = a + bi$ (a, b 实数) 总是有解的；这就是說，这个域中每个数都在域中有一个"平方根".

証明. 数 $x = c + di$(c, d 实数)具有所要的性质当且仅当

$$(c+di)^2 = a + bi,$$

这就是說，满足条件

$$c^2 - d^2 = a, \quad 2cd = b.$$

由这些方程推出：$(c^2+d^2)^2 = a^2+b^2$，从而 $c^2+d^2 = \sqrt{a^2+b^2}$. 再根据第一个条件我們决定 c^2 与 d^2：

$$c^2 = \frac{a+\sqrt{a^2+b^2}}{2},$$

$$d^2 = \frac{-a+\sqrt{a^2+b^2}}{2}.$$

右端的数实际上是 $\geqslant 0$. 因之，除符号外我們可以定出 c 与 d. 相乘即得

$$4c^2d^2 = -a^2 + (a^2+b^2) = b^2;$$

因之由后一个条件

$$2cd = b$$

可以定出 c 与 d 的符号.

由所証的結論推知,在复数域中二次方程

$$x^2 + px + q = 0$$

是可解的,只要把它化成形式

$$\left(x + \frac{p}{2}\right)^2 = \frac{p^2}{4} - q.$$

因之,解是

$$x = -\frac{p}{2} + w,$$

这里 w 表示方程 $w^2 = \frac{p^2}{4} - q$ 的任一个解.

"代数基本定理",更恰当些称为复数理論的基本定理,說明了在域 Ω 中不但是二次方程,并且每个非常数的多項式 $f(z)$ 都有零点.

基本定理最簡单的証明可能是函数論的証明,它是这样的:假設多項式 $f(z)$ 沒有复的零点,那么

$$\frac{1}{f(z)} = \varphi(z)$$

就是一个在整个 z-平面上正則的函数,而当 $z \to \infty$ 时它是有界的(甚至是趋向于零),因之根据 Liouville,它是一个常数;于是 $f(z)$ 也就是一个常数.

如果我們希望只假定函数論的最初步的知識,那么代替函数 $\varphi(z)$ 可以考慮同样是有理的函数

$$\psi(z) = \frac{\varphi(z) - \varphi(0)}{z},$$

它与 $\varphi(z)$ 一样也是在整个 z-平面上正則的. 这个函数沿半径为 R 的圓周 K 的积分应該等于零:

$$\int_K \frac{\varphi(z)-\varphi(0)}{z}dz = \int_0^{2\pi}\{\varphi(Re^{i\vartheta})-\varphi(0)\}id\vartheta = 0.$$

但是对于足够大的 R 有

$$|\varphi(Re^{i\vartheta})| < \varepsilon,$$

$$\left|\int_0^{2\pi}\varphi(Re^{i\vartheta})id\vartheta\right| < 2\pi\varepsilon,$$

而

$$\int_0^{2\pi}\varphi(0)id\vartheta = 2\pi i\varphi(0),$$

因之

$$|2\pi i\varphi(0)| < 2\pi\varepsilon, \quad \varphi(0)=0, \quad 1=f(0)\varphi(0)=0,$$

这是矛盾.

对于基本定理，Gauss 給了好几个証明. 在§71我們将看到 Gauss 的第二个証明，这个証明只用到实数与复数一些最簡单的性质，但是牽涉到困难的代数方法[1].

复数 $\alpha = a + bi$ 的**絕对值** $|\alpha|$ 定义为实数

$$|\alpha| = \sqrt{a^2+b^2} = \sqrt{\alpha\bar{\alpha}},$$

这里 $\bar{\alpha}$ 是共軛复数，即对于实数域的共軛数 $a - bi$.

显然有 $|\alpha| \geqslant 0$，并且只在 $\alpha = 0$ 时才有 $|\alpha| = 0$. 再则，$\sqrt{\alpha\beta\bar{\alpha}\bar{\beta}} = \sqrt{\alpha\bar{\alpha}}\cdot\sqrt{\beta\bar{\beta}}$，因而

$$|\alpha\beta| = |\alpha|\cdot|\beta|. \tag{1}$$

为了証明另一个关系

$$|\alpha+\beta| \leqslant |\alpha| + |\beta|, \tag{2}$$

我們暂时先假定特殊的关系

$$|1+\gamma| \leqslant 1 + |\gamma|. \tag{3}$$

如果 $\alpha = 0$，则 (2) 是显然的；如果 $\alpha \neq 0$，则

$$|\alpha+\beta| = |\alpha(1+\alpha^{-1}\beta)| = |\alpha|\,|1+\alpha^{-1}\beta|$$
$$\leqslant |\alpha|(1+|\alpha^{-1}\beta|) = |\alpha| + |\beta|.$$

---

1) 譬如在 C. Jordan: Cours d'Analyse I, 第三版, 202 頁可以找到另一个簡单的証明. H. Weyl 在 *Math. Z.*, **20** (1914), 142 頁上給了一个直观的証明.

为了証明(3)，令 $\gamma = a + bi$，有

$$|\gamma| = \sqrt{a^2 + b^2} \geqslant \sqrt{a^2} = |a|,$$

$$\begin{aligned} |1 + \gamma|^2 &= (1 + \gamma)(1 + \bar{\gamma}) = 1 + \gamma + \bar{\gamma} + \gamma\bar{\gamma} \\ &= 1 + 2a + |\gamma|^2 \leqslant 1 + 2|\gamma| + |\gamma|^2 \\ &= (1 + |\gamma|)^2, \end{aligned}$$

因之

$$|1 + \gamma| \leqslant 1 + |\gamma|,$$

这就証明了(3)，因而也証明了(2)。

§71. 实域的代数理論

有序域，特别是实的数域具有以下的性質，一个平方和只有在每一項为零时才会等于零，或者換个説法：-1 不能表成平方和[1]。复数域就沒有这个性質；因为 -1 本身就是一个平方。我們現在来証明，这个性質对于实的数域以及(在所有代数数的域中)与之共軛的域是特征性質，并且可以用来給出实代数数的域以及与之共軛的域的一个代数构造法。我們定义[2]：

一个域称为形式实的，如果 -1 不能表成平方和。

形式实域的特征一定是零；因为在特征 p 的域中 -1 是 $p-1$ 个平方項 1^2 的和。形式实域的子域显然也是形式实的。

域 $\mathbf{P}$ 称为实封閉的[3]，**如果 $\mathbf{P}$ 是形式实的，但是沒有 $\mathbf{P}$ 的眞代数扩张是形式实的。**

---

1) 如果在某一域中 -1 可以表成平方和 $\sum a_\nu^2$，于是 $1^2 + \sum a_\nu^2 = 0$；因之 0 是一些不全为零的平方項的和。反之，如果有 $\sum b_\nu^2 = 0$，其中有一个 $b_\lambda \neq 0$，那么用 b_λ^2 除每一項，再移項即得 $-1 = \sum a_\nu^2$。

2) 参看 E. Artin 与 O. Schreier: Algebraische Konstruktion reeller Körper (实域的代数构造)，*Abh. Math. Sem. Hamburg*, **5** (1926), 83—115。

3) 我們宁愿用簡短的名称"实封閉的"来代替更为确切的"实代数封閉的"。

定理 1. 每个实封闭的域有一种且只有一种方法定义成有序域.

設 **P** 是实封閉的. 我們要来証明:

如果 a 是 **P** 中一个非零元素, 那么 a 本身是一个平方或者 $-a$ 是一个平方, 这两个情形是互相排斥的. 在 **P** 中平方和一定是平方.

由此立即推出定理 1; 因为約定 $a>0$, 当 a 是平方且不为零, 显然定义了域 **P** 的一个順序, 并且这是唯一可能的定义, 因为在任何順序下平方一定是 $\geqslant 0$ 的.

如果 γ 不是 **P** 中元素的平方, $\sqrt{\gamma}$ 是多項式 $x^2-\gamma$ 的一个根, 那么 $\mathbf{P}(\sqrt{\gamma})$ 是 **P** 的一个眞代数扩张, 因而不是形式实的. 于是有方程

$$-1=\sum_{\nu=1}^{n}(\alpha_\nu\sqrt{\gamma}+\beta_\nu)^2$$

或者

$$-1=\gamma\sum_{\nu=1}^{n}\alpha_\nu^2+\sum_{\nu=1}^{n}\beta_\nu^2+2\sqrt{\gamma}\sum_{\nu=1}^{n}\alpha_\nu\beta_\nu,$$

这里 α_ν, β_ν 全属于 **P**. 其中最后一項一定为零, 否則 $\sqrt{\gamma}$ 就要屬于 **P** 了. 第一項不可能等于零, 否則 **P** 就不是形式实了. 由此首先推知, γ 在 **P** 中不可能表成平方和; 否則 -1 就表成了平方和. 这就是說, 如果 γ 不是平方, 那么它也就不是平方和. 换个說法: **P** 中每个平方和都是 **P** 中一个平方.

現在我們得到

$$-\gamma=\frac{1+\sum_{\nu=1}^{n}\beta_\nu^2}{\sum_{\nu=1}^{n}\alpha_\nu^2}.$$

这个表达式的分子与分母都是平方和，因而都是平方；也就是 $-\gamma=c^2$. c 属于 $\mathbf{P}$. 由此可見，$\mathbf{P}$ 中每个元素 γ 至少适合方程 $\gamma=b^2$ 与 $-\gamma=c^2$ 中的一个；但是当 $\gamma\neq 0$ 时，它不可能同时适合两个方程，否則就有 $-1=(b/c)^2$，这是不可能的.

根据定理 1，以后我們总是認为实封閉域是有序的.

定理 2. 在实封閉域中，每个奇次多項式至少有一个零点.

定理对一次多項式是显然的. 假定它对于 $<n$ 的奇次多項式已証；設 $f(x)$ 是一 n ($n>1$，奇数) 次多項式. 如果 $f(x)$ 在这个实封閉域 $\mathbf{P}$ 中可約，那么它至少有一个次数 $<n$ 的奇次不可約因子，因而在 $\mathbf{P}$ 中有一根. 由假定 $f(x)$ 不可約，我們現在来推出一个矛盾. 設 α 是 $f(x)$ 的一个形式添加的零点. $\mathbf{P}(\alpha)$ 不是形式实的；因之我們有方程

$$-1=\sum_{\nu=1}^{r}(\varphi_\nu(\alpha))^2, \tag{1}$$

这里 $\varphi_\nu(x)$ 是系数在 $\mathbf{P}$ 中次数最高为 $n-1$ 的多項式. 由(1)即得一恆等式

$$-1=\sum_{\nu=1}^{r}(\varphi_\nu(x))^2+f(x)g(x). \tag{2}$$

φ_ν^2 的和是偶次的，因为最高項系数都是平方，加起来不可能消掉，并且次数大于零，否則 (1) 就已經是矛盾. 因之 $g(x)$ 是一次数 $\leqslant n-2$ 的奇次多項式；由归納假定 $g(x)$ 在 $\mathbf{P}$ 中有一根 a. 把 a 代入 (2) 即得

$$-1=\sum_{\nu=1}^{r}(\varphi_\nu(a))^2,$$

这样就得出了矛盾. 因为 $\varphi_\nu(a)$ 全是 $\mathbf{P}$ 中元素.

定理 3. 实封閉的域不是代数封閉的. 但是在添加了 i 之

后所得的域[1]是代数封閉的.

前一半是显然的. 因为方程 $x^2+1=0$ 在每个形式实域中总是不可解的.

后一半由下面的定理立即推出.

定理 3a. 如果在一有序域 $\mathbf{K}$ 中,每个正元素都有一平方根并且每个奇次多項式都至少有一零点,那么在添加了 i 之后所得的域是代数封閉的.

我們首先指出,在 $\mathbf{K}(i)$ 中每个元素都有一平方根,因而每个二次方程都是可解的. 这个証明与 § 70 中对于复数域所作的完全一样.

根据 § 62,为了証明 $\mathbf{K}(i)$ 的代数封閉性我們只要証每个在 $\mathbf{K}$ 中不可約的多項式 $f(x)$ 都在 $\mathbf{K}(i)$ 中有根. 設 $f(x)$ 是一无重根的 n 次多項式,其中 $n=2^m q$, q 奇数. 我們来对 m 作归納法,假定每个系数在 $\mathbf{K}$ 中的无重根的多項式,它的次数被 2^{m-1} 整除,但不能被 2^m 整除,在 $\mathbf{K}(i)$ 中有根. (根据定理的假定,$m=1$ 时是对的.) 設 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是 $f(x)$ 在 $\mathbf{K}$ 的一个扩域中的根. 选择 $\mathbf{K}$ 中元素 c 使得 $\frac{n(n-1)}{2}$ 个式子 $\alpha_j\alpha_k+c(\alpha_j+\alpha_k)$ 对于 $1\leqslant j<k\leqslant n$ 全有不同的值. 因为这些式子在 $\mathbf{K}$ 中显然适合一个次数为 $\frac{n(n-1)}{2}$ 的方程,所以根据归納假定,其中至少有一个在 $\mathbf{K}(i)$ 中,譬如說 $\alpha_1\alpha_2+c(\alpha_1+\alpha_2)$. 按 c 所适合的条件,我們有(参看 § 43)

$$\mathbf{K}(\alpha_1\alpha_2, \alpha_1+\alpha_2)=\mathbf{K}(\alpha_1\alpha_2+c(\alpha_1+\alpha_2)),$$

因之 α_1 与 α_2 可以由在 $\mathbf{K}(i)$ 中解一个二次方程得出.

---

1) 在这里和以后,i 总是代表 x^2+1 的根.

由定理 3a 同时也推出，复数域是代数封閉的. 这就是"代数基本定理"(参看 § 70).

定理 3 的逆是:

定理 4. 如果一形式实域 $\mathbf{K}$ 在添加了 i 之后成一代数封閉域，那么 $\mathbf{K}$ 是实封閉的.

証明. 在 $\mathbf{K}$ 与 $\mathbf{K}(i)$ 之間沒有中間域，因之除 $\mathbf{K}$ 本身与 $\mathbf{K}(i)$ 之外 $\mathbf{K}$ 沒有其它的代数扩张. $\mathbf{K}(i)$ 不是形式实的，因为 -1 在它里面是一个平方. 因而 $\mathbf{K}$ 是实封閉的.

由定理 4 特别推出，实数域是实封閉的.

系数在一个实封閉域 $\mathbf{K}$ 中的方程 $f(x)=0$ 的根一定在 $\mathbf{K}(i)$ 中，如果它不包含在 $\mathbf{K}$ 中，那么出現的一定是一对共軛 (对于 $\mathbf{K}$) 根. 如果 $a+bi$ 是一根，那么共軛根是 $a-bi$. 如果在 $f(x)$ 的分解中把共軛的綫性因子合在一起，那么 $f(x)$ 就分解成在 $\mathbf{K}$ 中不可約的綫性与二次因子.

我們現在已經能够对于任意的实封閉域来証明关于多項式的"Weierstrass 零点定理".

定理 5. 設 $f(x)$ 是一系数在实封閉域 $\mathbf{P}$ 中的多項式，a, b 是 $\mathbf{P}$ 的元素，有 $f(a)<0$, $f(b)>0$，于是 $\mathbf{P}$ 中有一在 a 与 b 之間的元素 c 使 $f(c)=0$.

証明. 上面已經看到，$f(x)$ 在 $\mathbf{P}$ 中分解成綫性的与不可約二次的因子. 不可約二次多項式 x^2+px+q 在 $\mathbf{P}$ 中永远取正值；因为它可以写成 $\left(x+\frac{p}{2}\right)^2+\left(q-\frac{p^2}{4}\right)$，其中第一項一定 $\geqslant 0$ 而在不可約的假定下第二項是正的. 因之 $f(x)$ 的变号只可能是由某一綫性因子的变号造成，所以它在 a 与 b 之間有一个根.

根据这个定理，所有在 § 69 中由 Weierstrass 零点定理得出的

推論对实封閉域也成立，特別是关于实根的 Sturm 定理.

最后我們来証明

定理 6. 設 $\mathbf{K}$ 是一有序域，$\bar{\mathbf{K}}$ 是由 $\mathbf{K}$ 添加了所有 $\mathbf{K}$ 中正元素的平方根所得的域. $\bar{\mathbf{K}}$ 是形式实的.

显然只要証明，沒有形式为

$$(3)\qquad -1=\sum_{\nu=1}^{n} c_\nu \xi_\nu^2$$

的方程成立就行了，其中 c_ν 是 $\mathbf{K}$ 中正元素，ξ_ν 是 $\bar{\mathbf{K}}$ 中的元素. 假設有这样一个方程. 在这些 ξ_ν 中自然只能出現有限多个添加到 $\mathbf{K}$ 中的平方根，譬如說是 $\sqrt{a_1}, \sqrt{a_2}, \cdots, \sqrt{a_r}$. 在所有的方程 (3) 中我們可以选择一个使 r 有最小值的. [一定有 $r\geqslant 1$，因为在 $\mathbf{K}$ 中形式为(3)的方程不存在.] 每个 ξ_ν 可以表成 $\xi_\nu=\eta_\nu+\zeta_\nu\sqrt{a_r}$，其中 η_ν，ζ_ν 在 $\mathbf{K}(\sqrt{a_1}, \sqrt{a_2}, \cdots, \sqrt{a_{r-1}})$ 中. 于是我們有

$$(4)\qquad -1=\sum_{\nu=1}^{n} c_\nu\eta_\nu^2+\sum_{\nu=1}^{n} c_\nu a_r\zeta_\nu^2+2\sqrt{a_r}\sum_{\nu=1}^{n} c_\nu\eta_\nu\zeta_\nu.$$

如果 (4) 中最后一项为零，那么 (4) 就具有 (3) 的形式，但包含平方根的个数小于 r. 如果它不为零，那么 $\sqrt{a_r}$ 就在 $\mathbf{K}(\sqrt{a_1}, \cdots, \sqrt{a_{r-1}})$ 中，于是(3)可以改写，使其中出現的平方根的个数小于 r. 在任何情形下我們的假定都引出矛盾.

习题. 1. 全体代数数所成的域是代数封閉的，实代数数所成的域是实封閉的.

2. 按 § 62 純代数地构造的域 Γ 的代数封閉的代数扩域与代数数的域 $\mathbf{A}$ 同构.

3. 設 $\mathbf{P}$ 是一实的数域，Σ 是 $\mathbf{P}$ 上实的代数数的域. Σ 是实封閉的.

4. 如果 $\mathbf{P}$ 是形式实的，t 对于 $\mathbf{P}$ 是超越的，那么 $\mathbf{P}(t)$ 也是形式实的. [如果 $-1=\Sigma\varphi_\nu(t)^2$，那么用 $\mathbf{P}$ 中一个适当的元素来代 t.]

§ 72. 关于形式实域的存在定理

定理 7. 設 $\mathbf{K}$ 是一形式实域，Ω 是 $\mathbf{K}$ 上一代数封閉域. 于是在 $\mathbf{K}$ 与 Ω 之間(至少)有一实封閉域 $\mathbf{P}$ 使 $\Omega = \mathbf{P}(i)$.

證明. 我們可以假定 Ω 是良序的(§ 7). 这个良序必須与上一节所談的序区别开(Ω 不可能成一有序域，因为 -1 是一个平方)；因之当 a 在这个良序下前于 b，我們現在記为 $a <\circ b$.

我們令 Ω 中每个元素 a 与 Ω 的两个子域 $\mathbf{P}_a$, Σ_a 对应，它們按下面的遞归定义关系唯一决定：

1. $\mathbf{P}_a$ 是 $\mathbf{K}$ 与所有的 $\Sigma_b(b <\circ a)$ 的和.

2. $\Sigma_a = \mathbf{P}_a(a)$，当 $\mathbf{P}_a(a)$ 是形式实的，否則 $\Sigma_a = \mathbf{P}_a$.

最后我們定义 $\mathbf{P}$ 为所有 Σ_a 的和.

我們現在要来証明，所有的 $\mathbf{P}_a$ 以及 $\mathbf{P}$ 都是形式实的. 假定对于所有的 $\mathbf{P}_b$, $b <\circ a$, 結論已經成立(在討論 $\mathbf{P}$ 时就对所有的 $\mathbf{P}_b$ 作假定). 我們指出：如果 $\mathbf{P}_b$ 是形式实的，那么 Σ_b 也是(Σ_b 的定义). 假如 $\mathbf{K}$ 以及所有的 $\Sigma_b(b <\circ a)$ 是形式实的，那么它們的併 $\mathbf{P}_a$ 也是，因为如果在 $\mathbf{P}_a$ 中有一个表示 $-1 = \Sigma a_\nu^2$，那么这些 a_ν 一定全部属于某一个 Σ_b. 由超限归納法推出，所有的 $\mathbf{P}_b$ 是形式实的，从而 $\mathbf{P}$ 也是形式实的.

設 a 是 Ω 的一个元素，它不属于 $\mathbf{P}$. 于是 a 也就不属于 Σ_a，因而 $\mathbf{P}_a(a)$ 不是形式实的，当然 $\mathbf{P}(a)$ 也不是形式实的. 只有 a 对 $\mathbf{P}$ 是代数的才可能；因为形式实域的一个单純超越扩张还是形式实的(§ 71，习題 4). 因之 Ω 的每个元素对于 $\mathbf{P}$ 都是代数的，这就是說，Ω 对于 $\mathbf{P}$ 是代数的. 因为 a 可以取 $\mathbf{P}$ 以外的 Ω 中任意一个代数元素，所以 $\mathbf{P}$ 沒有单純眞代数扩张 $\mathbf{P}(a)$ 是形式实的，从而 $\mathbf{P}$ 是实封閉的. 按定理 3(§ 71)，$\mathbf{P}(i)$ 是代数封閉的，因而就是

Ω. 这就証明了定理.

注意. 在許多重要的特殊情形，Ω 是可数无穷的，因之不需要用良序定理. 例如，Ω 是代数数的域或者 Ω 对于这样的域只有有限的超越次数.

定理 7 的一些特殊情形以及直接推論还值得特别写一下.

定理 7a. 对于每个形式实域 $\mathbf{K}$ 都（至少）有一个实封閉的代数扩张.

只要在定理 7 中把 Ω 取作 $\mathbf{K}$ 的代数封閉的代数扩张就行了.

定理 7b. 每个形式实域可以按（至少）一种方法定义成有序域.

这个直接由定理 1（§ 71）与定理 7a 推出.

如果 Ω 是任意一个特征为零的代数封閉域，在定理 7 中取 $\mathbf{K}$ 为有理数域，那么就有

定理 7c. 每个特征为零的代数封閉域 Ω 都包含（至少）一个实封閉的子域 $\mathbf{P}$ 使 $\Omega = \mathbf{P}(i)$.

对于有序域，定理 7 可以加強为：

定理 8. 如果 $\mathbf{K}$ 是一有序域，那么 $\mathbf{K}$ 有一个，并且除去等价的扩张外只有一个实封閉的代数扩张 $\mathbf{P}$，它的順序是 $\mathbf{K}$ 的順序的一个开拓. $\mathbf{P}$ 除去单位自同构外沒有其它自同构保持 $\mathbf{K}$ 的元素不变.

証明. 和在定理 6 中一样，$\overline{\mathbf{K}}$ 表示由 $\mathbf{K}$ 添加 $\mathbf{K}$ 的所有正元素的平方根所得的域. 設 $\mathbf{P}$ 是 $\overline{\mathbf{K}}$ 的一个实封閉的代数扩张. 根据定理 7a 这样一个域是存在的，因为 $\overline{\mathbf{K}}$ 是形式实的. $\mathbf{P}$ 对于 $\mathbf{K}$ 是代数的并且 $\mathbf{P}$ 的順序是 $\mathbf{K}$ 的順序的一个开拓，因为 $\mathbf{K}$ 中正元素在 $\overline{\mathbf{K}}$ 中都是平方，在 $\mathbf{P}$ 中当然也是. 这就証明了这样一个域

P 的存在.

設 $\mathbf{P}^*$ 是 $\mathbf{K}$ 的第二个实封閉的代数扩张，它的順序也是 $\mathbf{K}$ 的一个开拓. 設 $f(x)$ 是系数在 $\mathbf{K}$ 中的一个(不一定不可約)多項式. Sturm 定理使我們在 $\mathbf{K}$ 中就可以断定 $f(x)$ 在 $\mathbf{P}$ 或者 $\mathbf{P}^*$ 中有多少个根. 我們所考察的 $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ 的 Sturm 組只有一个. 因之 $f(x)$ 在 $\mathbf{P}$ 中与 $\mathbf{P}^*$ 中根的个数相同. 特别地，$\mathbf{K}$ 中每个在 $\mathbf{P}$ 中有根的方程在 $\mathbf{P}^*$ 中一定也有根. 反之亦然. 假設 $\alpha_1, \alpha_2, \cdots, \alpha_r$ 是 $f(x)$ 在 $\mathbf{P}$ 中的根，$\beta_1^*, \beta_2^*, \cdots, \beta_r^*$ 是 $f(x)$ 在 $\mathbf{P}^*$ 中的根. 再假設 ξ 是 $\mathbf{P}$ 中这样一个元素，使 $\mathbf{K}(\xi) = \mathbf{K}(\alpha_1, \cdots, \alpha_r)$，而 $F(x) = 0$ 是 ξ 在 $\mathbf{K}$ 中的不可約方程. $F(x)$ 在 $\mathbf{P}$ 中有根 ξ，因而它在 $\mathbf{P}^*$ 中至少也有一个根 η^*; $\mathbf{K}(\xi)$ 与 $\mathbf{K}(\eta^*)$ 是 $\mathbf{K}$ 的等价的扩张. 因为 $\mathbf{K}(\xi)$ 是由 $f(x)$ 的 r 个根生成的，所以 $\mathbf{K}(\eta^*)$ 一定也是由 $f(x)$ 的 r 个根生成的; 現在 $\mathbf{K}(\eta^*)$ 是 $\mathbf{P}^*$ 的子域，所以有 $\mathbf{K}(\eta^*) = \mathbf{K}(\beta_1^*, \cdots, \beta_r^*)$. 因之 $\mathbf{K}(\alpha_1, \cdots, \alpha_r)$ 与 $\mathbf{K}(\beta_1^*, \cdots, \beta_r^*)$ 是 $\mathbf{K}$ 的等价扩张.

現在为了証明 $\mathbf{P}$ 与 $\mathbf{P}^*$ 是 $\mathbf{K}$ 的等价扩张，我們指出，$\mathbf{P}$ 到 $\mathbf{P}^*$ 的同构映射一定是保持順序的，因为它們的順序(按 §71 定理 1 的証明)是由是否平方这个性質刻划的. 我們来定义下面这个由 $\mathbf{P}$ 到 $\mathbf{P}^*$ 的映射 σ. 設 α 是 $\mathbf{P}$ 的一个元素，$p(x)$ 是它在 $\mathbf{K}$ 中的不可約多項式，$\alpha_1, \alpha_2, \cdots, \alpha_r$ 是 $p(x)$ 在 $\mathbf{P}$ 中的根，并且如此編号使 $\alpha_1 < \alpha_2 < \cdots < \alpha_r$; 而 $\alpha = \alpha_k$. 如果 $\alpha_1^*, \alpha_2^*, \cdots, \alpha_r^*$ 是 $p(x)$ 在 $\mathbf{P}^*$ 中的根并且 $\alpha_1^* < \alpha_2^* < \cdots < \alpha_r^*$，那么我們令 $\sigma(\alpha) = \alpha_k^*$. 显然 σ 是单值的并且保持 $\mathbf{K}$ 中元素不变. 現在需要証明 σ 是一同构映射. 为此，設 $f(x)$ 是 $\mathbf{K}$ 中任意一个多項式; $\gamma_1, \gamma_2, \cdots, \gamma_s$ 是它在 $\mathbf{P}$ 中的根; $\gamma_1^*, \gamma_2^*, \cdots, \gamma_s^*$ 是它在 $\mathbf{P}^*$ 中的根. 再設 $g(x)$ 是 $\mathbf{K}$ 中多項式，它的根是 $f(x)$ 的根的差的平方根. 設 $g(x)$ 在 $\mathbf{P}$

中的根是 $\delta_1, \delta_2, \cdots, \delta_t$; $\delta_1^*, \delta_2^*, \cdots, \delta_t^*$ 是它在 $\mathbf{P}^*$ 中的根. 根据以上的証明, $\Lambda = \mathbf{K}(\gamma_1, \cdots, \gamma_s, \delta_1, \cdots, \delta_t)$ 与 $\Lambda^* = \mathbf{K}(\gamma_1^*, \cdots, \gamma_s^*, \delta_1^*, \cdots, \delta_t^*)$ 是 $\mathbf{K}$ 的等价扩张. 因之由 Λ 到 Λ^* 有一保持 $\mathbf{K}$ 的元素不变的同构映射 τ. 在 τ 之下, 每个 γ 对应于一个 γ^*, 每个 δ 对应于一个 δ^*. 假設記号是如此选择, 使 $\tau(\gamma_k) = \gamma_k^*$, $\tau(\delta_h) = \delta_h^*$. 如果 $\gamma_k < \gamma_l$(在 $\mathbf{P}$ 中), 那么对某一指标 h 有 $\gamma_l - \gamma_k = \delta_h^2$, 因而 $\gamma_l^* - \gamma_k^* = \delta_h^{*2}$, 这就是說, $\gamma_k^* < \gamma_l^*$ (在 $\mathbf{P}^*$ 中). 因之 τ 按大小順序把 $f(x)$ 在 $\mathbf{P}$ 中与 $\mathbf{P}^*$ 中的根对应起来. 因为以上的关系对于 $f(x)$ 在 $\mathbf{K}$ 中的不可約因子的根也成立, 所以我們有 $\tau(\gamma_k) = \sigma(\gamma_k)(k = 1, 2, \cdots, s)$. 只要考虑到 $\mathbf{P}$ 中任意两个給定的元素 α, β 与 $\alpha + \beta$, $\alpha \cdot \beta$ 同时是 $f(x)$ 的根的情形, 我們就得出結論, σ 是 $\mathbf{P}$ 到 $\mathbf{P}^*$ 的一个同构映射, 并且是唯一保持 $\mathbf{K}$ 的元素不变的一个. 如果选择 $\mathbf{P}^* = \mathbf{P}$, 我們就得出定理中关于 $\mathbf{P}$ 的自同构的結論.

因为按 § 67, 有理数域 Γ 的順序是唯一的, 所以由定理 8 立即推出:

定理 8a. 在 Γ 上有一个且除去同构的域外只有一个实封閉的代数域.

对于这个域, 我們自然可以就取通常意义下的 (§ 68) 实代数数的域, 它是从实数中选出代数数組成的. 这是超越的途径, 我們可以由定理 7 給出的(取 $\mathbf{K} = \Gamma$, Ω 为 Γ 上的代数封閉的代数扩域 $\mathbf{A}$)純代数的构造法来避开它. 因之我們按純代数的途径造出了实代数数的域, 用 $\mathbf{P}$ 表示. 所有代数数的域具有形式 $\mathbf{A} = \mathbf{P}(i)$.

不过我們将看到, $\mathbf{P}$ 在 $\mathbf{A}$ 中不是唯一的实封閉域, 而是无穷多个等价域中的一个.

定理 9. Γ 的每个形式实的, 可数的, 代数扩域 $\mathbf{K}^*$ 都与 $\mathbf{P}$

的一个子域，也就是与一个实的代数数域同构。

証明． 根据定理 7a，对于 $\mathbf{K}^*$ 我們总可以造一个实封閉的代数扩域 $\mathbf{P}^*$，根据定理 8a，它一定与 $\mathbf{P}$ 同构。由此即得定理 9。

一个由 $\mathbf{K}^*$ 到 $\mathbf{K} \subseteq \mathbf{P}$ 的适当的同构映射自然也就給出 $\mathbf{K}^*$ 的一个适当的順序，因为 $\mathbf{P}$ 的所有子域 $\mathbf{K}$ 本来是有序的。反过来，$\mathbf{K}^*$ 的每个順序都可以由这个方法得出，因为在定理 9 的証明所造的那个实封閉的扩域 $\mathbf{P}^*$ 按定理 8 可以这样来造，使得它的順序与 $\mathbf{K}^*$ 的順序一致。在同构之下，这个順序变到 $\mathbf{P}$ 的（唯一可能的）順序。

我們特別取 $\mathbf{K}^*$ 为一个有限代数数域，它只有有限多个到 $\mathbf{A}$ 中的同构，于是即得：

把 $\mathbf{K}^*$ 变到实的代数数域的同构的个数等于 $\mathbf{K}^*$ 可能有的順序的个数（当 $\mathbf{K}^*$ 不是形式实的，个数为零）。

由 $\mathbf{A}$ 中每个形式实域都能扩充成一个实封閉域 $\mathbf{P}^* \subseteq \mathbf{A}$ 这个事实，我們得知，在 $\mathbf{A}$ 中有无穷多个这样的域 $\mathbf{P}^*$（按定理 8a，它們都是互相同构的）。因为当 n 为奇自然数，ζ 为 n 次单位根时，域 $\mathbf{K}_\zeta^* = \Gamma(\zeta\sqrt[n]{2})$ 与域 $\Gamma(\sqrt[n]{2})$ 同构，因而都是形式实的。它們的每一个都可以扩充到一个实封閉的扩域 $\mathbf{P}_\zeta^*$，这些域对于固定的 n 全不相同，因为一个有序域只能包含 2 的一个 n 次根。这些域的个数 n 可以取得任意地大。

习題． 1．設 ϑ 是 Γ 中不可約方程 $x^4 - x - 1 = 0$ 的一根。域 $\Gamma(\vartheta)$ 可以按几种方法定义成有序域？

2．設 t 是一不定元。域 $\Gamma(t)$ 能够按无穷多种方法定义成有序域，既可以是阿基米德的也可以不是。t 既可以成为无穷大元素也可以是无穷小元素（参看 §67，习題 1）。

3．当 t 是无穷小元素时，多項式 $(x^2 - t)^2 - t^3$ 在 $\Gamma(t)$ 的一个实封閉的扩域中有多少个根？根在什么范围內？

§73. 平 方 和

現在我們要来討論在一域 $\mathbf{K}$ 中哪些元素可以表成 $\mathbf{K}$ 中元素的平方和这个問題.

对于这个問題我們可以只限于討論形式实域. 假如 $\mathbf{K}$ 不是形式实的,那么 -1 是平方和,譬如:

$$-1 = \sum_{\nu=1}^{n} \alpha_\nu^2.$$

如果 $\mathbf{K}$ 的特征不为 2, 那么由此卽得, $\mathbf{K}$ 的任意元素 γ 都可以分解成 $n+1$ 个平方:

$$\gamma = \left(\frac{1+\gamma}{2}\right)^2 + \left(\sum \alpha_\nu^2\right)\left(\frac{1-\gamma}{2}\right)^2.$$

如果 $\mathbf{K}$ 的特征是 2,那么每个平方和本身就是平方:

$$\sum \alpha_\nu^2 = \left(\sum \alpha_\nu\right)^2,$$

这个問題也就解决了.

显然,平方和的和与积还是平方和. 平方和的商也是平方和:

$$\frac{\alpha}{\beta} = \alpha \cdot \beta \cdot (\beta^{-1})^2.$$

对于形式实的域 $\mathbf{K}$ 我們現在来証明下面的定理:

如果 γ 在 $\mathbf{K}$ 中不是平方和, 那么在 $\mathbf{K}$ 中可以定义一个順序使 γ 是負的.

証明. 設 γ 不是平方和. 我們首先証明, $\mathbf{K}(\sqrt{-\gamma})$ 是形式实的. 如果 $\sqrt{-\gamma}$ 在 $\mathbf{K}$ 中,結論是显然的. 否則:假如

$$-1 = \sum_{\nu=1}^{n} (\alpha_\nu\sqrt{-\gamma} + \beta_\nu)^2,$$

那么正如定理 1 (§ 71) 的証明一样可得:

$$\gamma = \frac{1 + \Sigma\beta_\nu^2}{\Sigma\alpha_\nu^2},$$

于是 γ 是平方和，与假設矛盾．因之 $\mathbf{K}(\sqrt{-\gamma})$ 是形式实的．如果按定理 7b(§72) 在 $\mathbf{K}(\sqrt{-\gamma})$ 中定义了一个顺序，那么 $-\gamma$ 作为平方一定是正的．这就証明了定理．

应用这个定理到形式实的代数数域（按 §72，这种域的所有可能的順序都可以由它到共軛的实的数域的同构映射得出）卽得：

代数数域 $\mathbf{K}$ 中元素 γ 是平方和当且仅当在把 $\mathbf{K}$ 变到共軛的实域的同构下，数 γ 不会变成負数．

当 $\mathbf{K}$ 不是形式实时，这个定理也成立，因为 $\mathbf{K}$ 的每个数都是平方和，而所要求的同构根本沒有．

在一代数数域 $\mathbf{K}$ 中，那些被把 $\mathbf{K}$ 变成共軛的实域的同构总是变到正数的数称 $\mathbf{K}$ 中的全正数．如果 $\mathbf{K}$ 沒有共軛的实域，那么 $\mathbf{K}$ 的每个数都称为全正的．全正的概念可以推广到任意域 $\mathbf{K}$ 上，$\mathbf{K}$ 中那些在每个可能的順序下都是正的数称为全正的．（如果 $\mathbf{K}$ 是不能序的，因而如果 $\mathbf{K}$ 不是形式实的，那么 $\mathbf{K}$ 的每个元素都是全正的．）于是这一节的結果可以总結为，在特征 $\neq 2$ 的域中，每个全正的元素都可以表成平方和．

关于第九章的文献

在 E. Landau: Über die Zerlegung total positiver Zahlen in Quadrate（关于全正数分解成平方和），Göttinger Nachr., 1919, 392 頁中有关于在数域中全正数表成的平方和中平方个数的定理．对于函数域的情形，可参看 D. Hilbert: Über die Darstellung definiter Formen als Summen von Formenquadraten（关于定形式表成平方形式的和），*Math. Ann.*, **32** (1888), 342—350，以及 E. Artin: Über die Zerlegung definiter Funktionen in Quadrate（关于定函数分解成平方和），*Abhandlungen aus dem Math. Seminar der Hamburgischen Universität*, **5** (1926), 100—115．关于代数基本定理可看最近的 J. G. van der Corput, Colloque international d'algèbre, Paris, Septembre 1949, Centre National Rech. scient., 或者更詳細的有 Math. Centrum 的 Scriptum 2, Amsterdam, 1950.

第十章 賦值域

§74. 賦　　值

§68 中所給出的由一个給定的有序域 $\mathbf{K}$ 作出域 Ω 的作法，并沒有完全利用到域 $\mathbf{K}$ 中的順序，而仅利用到域元素 a 的絕对值 $|a|$ 的順序． 这就使我們想到作更进一步的研究，将这一作法拓广到有序域以外的其它域去，祇要这种域中存在着具有絕对值的性質的一个函数 $\varphi(a)$．

一个域 $\mathbf{K}$ 称为**賦值域**，如果对 $\mathbf{K}$ 中的元素 a 定义了一个函数 $\varphi(a)$，它具有下面的性質：

1. $\varphi(a)$ 是某一有序域中的元素．
2. 对 $a \neq 0$ 有 $\varphi(a) > 0$；$\varphi(0) = 0$．
3. $\varphi(ab) = \varphi(a)\varphi(b)$．
4. $\varphi(a+b) \leqslant \varphi(a) + \varphi(b)$．

由 2. 和 3. 立即可以推出：

$$\varphi(1) = 1, \quad \varphi(-1) = 1, \quad \varphi(a) = \varphi(-a).$$

在 4. 中命 $c = a + b$ 可得

$$\varphi(c) - \varphi(a) \leqslant \varphi(c - a).$$

另一方面，由同樣方式可得

$$\varphi(a) - \varphi(c) \leqslant \varphi(c - a).$$

因此我們有

$$|\varphi(c) - \varphi(a)| \leqslant \varphi(c - a).$$

当 b 被换成 $-b$ 时，不等式 4. 也成立，这样我們就得到

$$\varphi(a-b) \leqslant \varphi(a)+\varphi(b).$$

利用完全归納法很容易将 4. 中的不等式推广到 n 个項的和.

如果 $\mathbf{K}$ 本身是一个有序域，并命 $\varphi(a)=|a|$，則性质 1. 至 4. 成立. 每个域都有一个"不足道"的賦值：$\varphi(a)=1$，当 $a \neq 0$；$\varphi(0)=0$. 但也存在着完全另外一种类型的賦值. 設 Γ 是有理数域. 設 p 是某一固定的素数，并将每个有理数 $a \neq 0$ 写成

$$a=\frac{s}{t} p^{n}$$

的形式，其中 s 和 t 是不能被 p 整除的整数，那末令

$$\varphi_{p}(a)=p^{-n}, \quad \varphi_{p}(0)=0$$

就可定义 Γ 的一个賦值. 1. 至 3. 非常容易驗証.

代替 4.，我們有更強的不等式

$$\varphi_{p}(a+b) \leqslant \max (\varphi_{p}(a), \varphi_{p}(b)). \tag{1}$$

事实上，設

$$a=\frac{s}{t} p^{n}, \quad b=\frac{u}{v} p^{m}, \quad s, t, u, v \text{ 与 } p \text{ 互素},$$

并設 $\varphi_{p}(b) \geqslant \varphi_{p}(a)$，即 $n \geqslant m$，則有

$$a+b=\frac{s v p^{n-m}+t u}{t v} p^{m},$$

因而

$$\varphi_{p}(a+b)=p^{-m'}, \quad \text{其中} \quad m' \geqslant m,$$

即

$$\varphi_{p}(a+b) \leqslant \varphi_{p}(b).$$

这就是 Γ 的 p-adic **賦值**.

p-adic 賦值的概念不难加以推广. 設 $\mathfrak{o}$ 是一个整环，$\mathbf{K}$ 是它

的商域，$\mathfrak{p}$ 是 $\mathfrak{o}$ 中一个具有下列性質的素理想：A. 各个幂 $\mathfrak{p},\mathfrak{p}^2,\cdots$ 互不相同，且其交为零理想. B. 設 $\mathfrak{o}$ 中的 a 恰被 $\mathfrak{p}^\alpha$ 整除，即能被 $\mathfrak{p}^\alpha$ 整除但不能被 $\mathfrak{p}^{\alpha+1}$ 整除，而 b 恰被 $\mathfrak{p}^\beta$ 整除，则 ab 恰被 $\mathfrak{p}^{\alpha+\beta}$ 整除. 这里 $\mathfrak{p}^\alpha$ 表示所有和 $\sum_\nu p_{\nu1}p_{\nu2}\cdots p_{\nu\alpha}$ 的全体，而所有的 $p_{\nu\kappa}$ 都是 $\mathfrak{p}$ 中元素. 特别 $\mathfrak{p}^1=\mathfrak{p}$，$\mathfrak{p}^0=\mathfrak{o}$. 現在我們給出如下的定义：設 $\mathfrak{o}$ 中的元素 a 恰被 $\mathfrak{p}^\alpha$ 整除，则命

$$\varphi(a)=e^{-\alpha},\quad \text{而}\quad \varphi(0)=0,$$

其中 e 是任意一个 >1 的实数. 这样，賦值 $\varphi(a)$ 就对 $\mathfrak{o}$ 中的元素有了定义，并且具有性質 1. 至 4.

另一方面，当一个賦值对整环中的元素有了定义时，由

$$\varphi\left(\frac{a}{b}\right)=\frac{\varphi(a)}{\varphi(b)}$$

立即可以将它开拓到商域中的元素上去. 这样一个定义是单值的，因为由

$$\frac{a}{b}=\frac{c}{d}\quad \text{或}\quad ad=bc$$

即有

$$\varphi(a)\varphi(d)=\varphi(b)\varphi(c)\quad \text{或}\quad \frac{\varphi(a)}{\varphi(b)}=\frac{\varphi(c)}{\varphi(d)}.$$

其次，賦值 $\varphi\left(\frac{a}{b}\right)$ 也具有性質 1. 至 4.. 头三个性質是自明的. 性質 4. 可証明如下：

$$\varphi\left(\frac{a}{b}+\frac{c}{d}\right)=\frac{\varphi(ad+bc)}{\varphi(bd)}\leqslant\frac{\varphi(ad)+\varphi(bc)}{\varphi(bd)}=$$
$$=\varphi\left(\frac{a}{b}\right)+\varphi\left(\frac{c}{d}\right).$$

这样，我們就从整环 $\mathfrak{o}$ 中由素理想 $\mathfrak{p}$ 所确定的賦值出发得出

了商域 **K** 的一个賦値．这个賦値称为 **K** 的 $\mathfrak{p}$-adic 賦値．

性質 A．和 B．对許多素理想成立．例如在一个具有唯一因子分解的环中，所有素主理想都具有这两个性質．在多項式环 $\Delta[x_1, \cdots, x_n]$ 中，理想

$$\mathfrak{p} = (x_1, \cdots, x_n)$$

也具有性質 A．和 B．．这样得出来的賦値 $\varphi(f)$ 即 $e^{-\alpha}$，其中 α 是出現在 f 中的最低次項的次数．

习題． 1．在賦値的定义中去掉 $\varphi(a)$ 不取負値的要求，証明：如果在 **K** 中有一个元素 c，使得 $\varphi(c) < 0$，則 $a \to \varphi(a)$ 是把 **K** 映成値域 **P** 的一个子域的一个同构映射．[将不等式 4．应用于 $\varphi(ac + bc)$，从而証明 4．中的等号成立．]

2．在 $\mathfrak{p}$-adic 賦値的情形下，条件 4．可改进为 (1)．

賦値域的一些最重要的研究，都是和値域 **P** 为阿基米德有序域的情形有关的．在这一情形下，根据 §68 的习題 2，**P** 可以嵌到实数域中去．因此我們从現在起假定値 $\varphi(a)$ 都是实数．在这里我們假定讀者知道实数的（自然）对数，对数的一些最簡单的性質以及一个正数 α 以任意实数为指数的冪 α^β．

此外，我們还要用到下面这样一个关于实数的引理：

如果 α, β, γ 是任意正实数，且对任意自然数 ν 有

$$\gamma^\nu \leqslant \alpha\nu + \beta,$$

則 $\gamma \leqslant 1$．

証明． 設 $\gamma = 1 + \delta$，$\delta > 0$，那末当 $\nu \geqslant 2$ 时将有

$$\gamma^\nu = (1+\delta)^\nu = 1 + \nu\delta + \frac{1}{2}\nu(\nu-1)\delta^2 + \cdots > \nu\delta + \frac{1}{2}\nu(\nu-1)\delta^2.$$

但当 ν 足够大时，必有

$$\nu\delta > \beta \quad 和 \quad \frac{1}{2}(\nu-1)\delta^2 > \alpha,$$

故得

$$\gamma^{\nu} > \beta + \alpha\nu,$$

而这是与所設相违的。

域 **K** 的一个实数賦值 $\varphi(a)$ 称为非阿基米德的，如果对单位元素的任意整数倍 $n = 1 + 1 + 1 + \cdots + 1$ 有

$$\varphi(n) \leqslant 1.$$

有理数域 Γ 的 p-adic 賦值就是一个非阿基米德賦值。 在这里值域为阿基米德域这一事实不起任何作用。

域 **K** 的賦值 φ 为非阿基米德賦值，当且仅当代替 4. 有更強的不等式

4'. $$\varphi(a + b) \leqslant \max(\varphi(a), \varphi(b))$$

成立。

証明. 1. 如果 4.' 对两个被加項的情形成立，那末相应的不等式对 n 个項的和也成立. 特别对于 $n = 1 + 1 + \cdots + 1$ 有

$$\varphi(n) \leqslant \max(\cdots, \varphi(1), \cdots) = 1.$$

2. 如果 φ 是非阿基米德賦值，則当 $\nu = 1, 2, 3, \cdots$ 时，

$$\begin{aligned}(\varphi(a + b))^{\nu} = \varphi((a + b)^{\nu}) &= \varphi\left(a^{\nu} + \binom{\nu}{1}a^{\nu-1}b + \cdots + b^{\nu}\right)\\ &\leqslant \varphi(a)^{\nu} + \varphi(a)^{\nu-1}\varphi(b) + \cdots + \varphi(b)^{\nu}\\ &\leqslant (\nu + 1)M^{\nu},\end{aligned}$$

其中 $M = \max(\varphi(a), \varphi(b))$. 根据前面的引理从这里可知

$$\frac{\varphi(a + b)}{M} \leqslant 1, \quad 即 \quad \varphi(a + b) \leqslant M.$$

这就証明了 4'.

在今后，即使值域 **P** 不是由实数組成的，我們也把不等式 4'. 看作是一个非阿基米德賦值的标志。 正如 Krull 所指出的那样，在这一場合下，可以取任意有序 Abel 羣作为取値范围，因为我們

只需要将不同的值相乘，以及比較值的大小，不同值相加的运算根本不会遇到.

下面的一点注記經常是很有用的，这个注記适用于所有在上面定义的意义下的非阿基米德賦值.

如果 $\varphi(a)$ 和 $\varphi(b)$ 不相等，則 4′. 中等号成立.

証明. 不妨設 $\varphi(a)>\varphi(b)$. 我們要証明

$$\varphi(a+b)=\varphi(a).$$

假如

$$\varphi(a+b)<\varphi(a),$$

那末 $\varphi(a+b)$ 和 $\varphi(-b)=\varphi(b)$ 都小于 $\varphi(a)$. 但这是和不等式

$$\varphi(a)\leqslant\max(\varphi(a+b),\varphi(-b))$$

相矛盾的.

对于非阿基米德賦值，引进另外一种記法經常是比較方便的(在文献中也常是这样作的). 我們不直接考慮实数值 $\varphi(a)$，而考慮指数 $w(a)=-\log\varphi(a)$. 考慮指数时，賦值的定义关系将成为:

1. 当 $a\neq 0$ 时，$w(a)$ 是一个实数.
2. $w(0)$ 是記号 ∞.
3. $w(ab)=w(a)+w(b)$.
4. $w(a+b)\geqslant\min(w(a),w(b))$.

在这种場合下我們就說所考慮的賦值是一个指数賦值. 我們之所以能够过渡到考慮指数，是由于較強的不等式 4′. 使得我們沒有必要将值 $\varphi(a)$ 相加. 对数变换倒轉了值的順序并将乘法改变为加法.

例. 設域 K 中的元素是 z-平面上的，或者更一般些，是某

一 Riemann 面上一个区域中的单値解析（亚純）函数．我們取 Riemann 面上一个固定的点 P，并作如下的定义：函数 a 的賦値 $w(a)$ 等于 α，如果它以 P 点为一个 α 阶零点；等于零，如果它在 P 点取不等于零的有限値；等于 $-\alpha$，如果它以 P 点为 α 阶极点．这时性质 1. 至 4. 都能成立．这样一来，相应于每个点 P 都有域 $\mathbf{K}$ 的一个賦値．这个例子說明賦値論在一个复变量的代数函数論中的意义．同时也說明了为什么我們常把域 $\mathbf{K}$ 的一个賦値称为一个"位"．

我們将指数賦値分为两种类型．离散賦値：这种賦値的特征是存在一个最小的正値 $w(a)$，而所有其它可能出現的値 $w(a)$ 都是它的整数倍（参看上面的例子）；非离散賦値：在这种賦値中可能出現的値 $w(a)$ 能够和値零接近到任意程度．由于一个値 $w(a)$ 的整数倍仍是一个値 $nw(a) = w(a^n)$，故在非离散賦値的情形下値 $w(a)$ 在实数集合中到处稠密．

有理数域的 p-adic 賦値是离散的，所有的 $\mathfrak{p}$-adic 賦値也同样是离散的．

在一个指数賦値的域 $\mathbf{K}$ 中，满足条件 $w(a) \geqslant 0$ 的元素組成一个环 $\mathfrak{I}$．事实上，由 $w(a) \geqslant 0$ 和 $w(b) \geqslant 0$ 可得 $w(a \pm b) \geqslant \min(w(a), w(b)) \geqslant 0$ 和 $w(ab) = w(a) + w(b) \geqslant 0$．$\mathbf{K}$ 中满足条件 $w(a) > 0$ 的元素的全体 $\mathfrak{p}$ 是 $\mathfrak{I}$ 中的一个素理想．事实上，首先由 $w(a) > 0$，$w(b) > 0$ 可得 $w(a \pm b) \geqslant \min(w(a), w(b)) > 0$，因而 $\mathfrak{p}$ 是一个模．其次，由 $a \in \mathfrak{p}$，即 $w(a) > 0$ 和 $w(c) \geqslant 0$ 可得 $w(ca) = w(c) + w(a) > 0$，故 $\mathfrak{p}$ 是一个理想．最后，由 $ab \equiv 0 (\mathrm{mod}\ \mathfrak{p})$，即由 $w(ab) = w(a) + w(b) > 0$ 可知 $w(a)$ 和 $w(b)$ 二数中至少必有一个为正，也就是說，a 和 b 两个元素中必有一个可被 $\mathfrak{p}$ 整除．$\mathfrak{p}$ 是一个素理想．

$\mathfrak{S}$ 称为赋值 w 的赋值环. $\mathfrak{S}$ 中的元素称为整元素(相对于赋值 w 来說的). 如果 a/b 是整元素,即 $w(a) \geqslant w(b)$, 我們就說元素 a 能被元素 b 整除(相对于赋值 w 来說).

满足条件 $w(a)=0$ 的元素就是环 $\mathfrak{S}$ 中的可逆元素. 由于 $\mathfrak{S}$ 中不属于 $\mathfrak{p}$ 的元素都是可逆元素,故 $\mathfrak{p}$ 是 $\mathfrak{S}$ 中的一个极大理想. 这样一来,同余类环 $\mathfrak{S}/\mathfrak{p}$ 就是一个域,称为赋值 w 的赋值商域. 如果域 $\mathbf{K}$ 的特征是 p, 則赋值商域的特征也是 p. 如果域 $\mathbf{K}$ 的特征为零,則赋值商域的特征可以是零(特征相等的情形),也可以是某一素数(特征不相等的情形). 特征不相等情形的一个典型的例子就是 p-adic 赋值. 如果我們将一个不定元添加到有理数域上去,并将一个有理函数的指数赋值定义为分母的次数和分子的次数之差,那末就得到特征相等情形的一个例子. 多项式环 $\mathbf{K}[x_1, \cdots, x_n]$ 中通过一个素理想定义的 $\mathfrak{p}$-adic 赋值(参看上文)也属于特征相等的情形.

关于这些概念的进一步討論,直到所有赋值的完全分类,可参看 H. Hasse, F. K. Schmidt, O. Teichmüller 和 E. Witt[1] 的工作. 关于赋值概念的推广可参看 K. Mahler 和 W. Krull 的工作[2].

习题. 3. 証明: $\mathfrak{S}$ 中的每个理想或者是所有满足条件 $w(a)>\delta$ 的元素 a 的集合, 或者是所有满足条件 $w(a)\geqslant\delta$ 的元素的集合, 其中 δ 为一非負实数. 对于离散赋値可以仅限于 $\geqslant$ 的情形,而其中的 δ 則是一个的确在值的集合中出現的数. 在非离散赋值的情形 δ 由理想所唯一确定.

4. 在离散赋值的情形 $\mathfrak{S}$ 中所有的理想都是 $\mathfrak{p}$ 的幂. 与此相反,在非离

1) Witt, E.: *J. reine u. angew. Math.*, **176** (1936) 126—140 以及所引文献.

2) Mahler, K.: Über Pseudobewertungen, I., *Acta Math.*, **66** (1936), 79—199; Ia. *Akad Wetensch. Amsterdam, Proc.*, **39** (1936), 57—65; II. *Acta Math.*, **67** (1936), 51—80. —Krull, W.: Allgemeine Bewertungstheorie, *J. reine angew. Math.*, **167** (1932), 160—196.

散賦值的情形 $\mathfrak{p}$ 的各次冪都和 $\mathfrak{p}$ 相等.

§75. 完备扩张

对于每个賦值域 **K**，我們可以利用 § 68 中所述的程序作出一个扩域 $\Omega_{\mathbf{K}}$，使得在它里面 Cauchy 收斂定理成立. 为了这个目的，首先必須由值域 **P** 作出相应的有序域 $\Omega_{\mathbf{P}}$，这个域将作为 $\Omega_{\mathbf{K}}$ 的值域之用. 現在我們通过下面的性質定义 **K** 中的一个基本叙列 $\{a_\nu\}$：

$$\varphi(a_p - a_q) < \varepsilon, \quad 当 \quad p > n(\varepsilon), \quad q > n(\varepsilon),$$

其中 ε 是 **P** 中任意一个正量. 由基本叙列环可以作出同余类域 $\Omega_{\mathbf{K}}$，其作法和 § 68 中的作法完全相同，所有的証明也可以逐字逐句借用. 唯一的差别就是現在的域 **K** 和域 $\Omega_{\mathbf{K}}$ 不再是有序的，而仅是賦值的. $\Omega_{\mathbf{K}}$ 的賦值定义如下：如果 α 由基本叙列 $\{a_\nu\}$ 决定，那末根据前面已經証明的不等式

$$|\varphi(a_\nu) - \varphi(a_\mu)| \leqslant \varphi(a_\nu - a_\mu),$$

值 $\varphi(a_\nu)$ 也构成 **P** 中的一个基本列，因而在 $\Omega_{\mathbf{P}}$ 中有一个极限 ω. 我們命

$$\varphi(\alpha) = \omega$$

具有同一极限 α 的基本叙列决定同一值 $\varphi(\alpha)$，这个值滿足要求 1. 至 4.

相对于賦值 φ 来說域 $\Omega_{\mathbf{K}}$ 是完备的，也就是說，Cauchy 收斂准則成立：

$\Omega_{\mathbf{K}}$ 中的每个基本叙列在 $\Omega_{\mathbf{K}}$ 中有极限.

我們說一个叙列 $\{a_\nu\}$ 是一基本叙列，如果对值域中的任意 $\varepsilon > 0$ 可以找到一个 n，使得当 $p > n$, $q > n$ 时

$$\varphi(a_p - a_q) < \varepsilon.$$

在非阿基米德賦值的情形，代替这样一个条件只須要求当 $\nu > n(\varepsilon)$ 时

$$\varphi(a_{\nu+1} - a_\nu) < \varepsilon$$

就够了。

事实上，$a_p - a_q$ 是 $|p-q|$ 个項 $a_{\nu+1} - a_\nu$ 的和，如果所有这些項的値都 $< \varepsilon$，則根据 §74(1)，它們的和的值也 $< \varepsilon$。

因此：

在一个完备的非阿基米德賦值域中，只要差 $a_{\nu+1} - a_\nu$ 构成一个零叙列，叙列 $\{a_\nu\}$ 就有极限。

这个准則也可以叙述如下：无穷級数 $a_1 + a_2 + a_3 + \cdots$ 收斂的充分必要条件是 $\lim a_\nu = 0$。

在下面我們仅限于考慮值为实数的情形。这时值域 $\mathbf{P}$ 就是一个实的数域而 Ω 則是实数域。从現在起我們可以假定 $\mathbf{P} = \Omega$。

如果我們用普通的絕对值来給有理数域 Γ 賦值：$\varphi(a) = |a|$，那末所得到的完备扩张自然就是实数域。如果我們从 Γ 的 p-adic 賦值出发，則所得到的完备扩张就是 Hensel 的 p-adic 数域 Ω_p。

这样，域 $\Omega_2, \Omega_3, \Omega_5, \Omega_7, \Omega_{11}, \cdots$ 就是一批在实数域之外的同等的完备域（对于算术理論来說，也是同样重要的）。

域 Ω_p 中的元素，即 p-adic 数，除了可以表成基本叙列之外，还有一种更加方便的表示方法。对 $\lambda = 0, 1, 2, 3, \cdots$ 我們考慮分子能被 p^λ 整除而分母不能被 p 整除的有理数，即滿足条件 $\varphi(a) \leqslant p^{-\lambda}$ 的有理数所組成的模 $\mathfrak{M}_\lambda$。如果两个有理数之差属于 $\mathfrak{M}_\lambda$，我們就說这两个数同余 $(\mathrm{mod}\ p^\lambda)$。現在設 $\{r_\mu\}$ 是一个由有理数組成的 p-adic 基本叙列，那末对于每个 λ 从某一足数 $n = n(\lambda)$ 起将会有

$$\varphi(r_\mu - r_\nu) \leqslant p^{-\lambda}, \quad 当 \quad \mu > n(\lambda), \ \nu > n(\lambda),$$

即有

$$r_\mu \equiv r_\nu (\bmod p^\lambda).$$

因此，当 $\mu > n(\lambda)$ 时，所有的数 r_μ 都属于模 $\mathfrak{M}_\lambda$ 的同一个同余类 $\mathfrak{R}_\lambda$. 这样，基本叙列 $\{r_\mu\}$ 决定一个同余类的叙列：

$$\mathfrak{R}_0 \supset \mathfrak{R}_1 \supset \mathfrak{R}_2 \supset \mathfrak{R}_3 \supset \mathfrak{R}_4 \supset \cdots,$$

这些同余类象这里所写出的那样，是一个包含在另一个之內的. 反之，如果一个叙列 $\{r_1, r_2, \cdots\}$ 决定出模 $\mathfrak{M}_\lambda$ 的同余类 $\mathfrak{R}$ 的一个包含在另一个之內的一个同余类叙列 $\{\mathfrak{R}_\lambda\}$，使得

$$r_\mu \in \mathfrak{R}_\lambda \quad \text{对所有} \quad \mu > n(\lambda),$$

那末它就是一个基本叙列.

特別，如果 $\{r_\mu\}$ 是零基本叙列，那末 $\mathfrak{R}_\lambda = \mathfrak{M}_\lambda$ 就是零同余类. 两个基本叙列相加时：$\{r_\mu\} + \{s_\mu\} = \{r_\mu + s_\mu\}$，相应的同余类叙列也相加：$\{\mathfrak{R}_\lambda + \mathfrak{S}_\lambda\}$. 特別，当我們把一个零基本叙列加到另一个基本叙列上去时，相应的同余类叙列不改变. 反之，如果两个基本叙列属于同一个同余类叙列 $\{\mathfrak{R}_\lambda\}$，則它們的差是零基本叙列. 因此，**每給一个 p-adic 数 $\alpha = \lim r_\nu$ 有一个上述类型的同余类叙列和它一一地相对应.**

将 p-adic 数表成同余类叙列，这就是上面所提到的比較方便的表示方法. 为了从 p-adic 数 α 的同余类叙列表示得出它的一个(特殊的)基本叙列，只要从每个同余类 $\mathfrak{R}_\lambda$ 中取出一个数 r'_λ 就行：这时必有 $\alpha = \lim r'_\lambda$. α 也可以表成一个无限和：命

$$r'_1 = s_0, \quad r'_{\lambda+1} - r'_\lambda = s_\lambda p^\lambda,$$

則

$$r'_{\lambda+1} = s_0 + s_1 p + s_2 p^2 + \cdots + s_\lambda p^\lambda,$$

因此

$$\alpha = \lim_{\lambda \to \infty} \sum_{\nu=0}^{\lambda} s_\nu p^\nu = \sum_{\nu=0}^{\infty} s_\nu p^\nu. \tag{1}$$

这里的 $s_1, s_2, \cdots$ 是分母不能被 p 整除的有理数。

普通整数的 p-adic 极限称为 p-adic 整数. 对同余类 $\mathfrak{R}_0, \mathfrak{R}_1, \cdots$ 来説，这就意味着每个这样的同余类当中都可以找到一个整数. 特别,在 p-adic 整数的情形, $\mathfrak{R}_0$ 就是零同余类 $\mathfrak{M}_0$, 即分母不能被 p 整除的有理数的全体. 另一方面，这一条件也是使得一个 p-adic 数为 p-adic 整数的充分条件:如果 $\mathfrak{R}_0$ 是模 $\mathfrak{M}_0$ 的零同余类，则所有同余类 $\mathfrak{R}_1, \mathfrak{R}_2, \cdots$ 包含有整数. 事实上, $\mathfrak{R}_\lambda$ 包含在 $\mathfrak{R}_0$ 之内,因而完全由形为 $\frac{r}{s}$, $s \not\equiv 0 \pmod p$ 的数組成. 解同余式

$$sx \equiv r \pmod{p^\lambda},$$

則有

$$x - \frac{r}{s} = \frac{sx - r}{s} \equiv 0 \pmod{\mathfrak{M}_\lambda}$$

因此整数 x 属于同余类 $\mathfrak{R}_\lambda$.

由于这个原因,当 α 为 p-adic 整数时, 在級数表示(1)中可取所有的 r'_λ,因而可取所有的 s_λ 为普通整数. 这样一来, (1) 就是 p 的一个带整系数的冪級数. 每个这样的冪級数都在 p-adic 賦值的意义下收斂,因而表示一个 p-adic 整数.

具有同余类叙列表示$\{\mathfrak{R}_0, \mathfrak{R}_1, \cdots\}$的每个 p-adic 数 α 都可以乘上 p 的一个冪成为一个 p-adic 整数. 事实上,設 r'_0 是同余类 $\mathfrak{R}_0$ 中的一个元素,那末将 r'_0 和 p 的一个冪 p^m 相乘之后, 可使得 $p^m r'_0$ 的分母不再含有因子 p,即 $p^m r'_0$ 属于模 $\mathfrak{M}_0$ 的零同余类. 現在如果将 p-adic 整数 $p^m\alpha$ 展成带有整系数 $s_0, s_1, \cdots$ 的冪級数 (1),就可得到 α 的一个冪級数表示,其中出現有限多个带負指数的項:

(2) $$\alpha = a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots$$

p-adic 整数 α 的表示式 (1) 可加以規范化, 即每次都取 r'_λ 为同余类 $\mathfrak{R}_\lambda$ 中最小的非負整数. 这时所有整数 s_ν 都滿足条件 $0 \leqslant s_\nu < p$.

現在再由(1)过渡到(2)，我們就得到每个 p-adic 数的一个唯一地确定的展开式(2)，其中 $0 \leqslant a_\nu < p$.

由 p-adic 数的表示式(2)立即可以看出，Ω_p 中的 p-adic 賦值的賦值环恰由所有 p-adic 整数組成. 因此，§ 74 中所引入的"整"元素的概念和"p-adic 整数"这一名称彼此吻合.

在 § 74 中我們曾經描述过怎样由一个整环 $\mathfrak{o}$ 中的素理想 $\mathfrak{p}$ 定义一个域 $\mathbf{K}$ 中的一个 $\mathfrak{p}$-adic 賦值. 由这个 $\mathfrak{p}$-adic 賦值可以得出一个完备的 $\mathfrak{p}$-adic 域 $\Omega_\mathfrak{p}$，这就是 Hensel p-adic 域的一个推广. 举例来說，如果 $\mathfrak{p}$ 是多項式整环 $\Delta[x]$ 中的理想 $(x-c)$，則 $\Omega_\mathfrak{p}$ 就是所有冪級数

(3) $\quad \alpha = a_{-m}(x-c)^{-m} + \cdots + a_0 + a_1(x-c) + a_2(x-c)^2 + \cdots$

的域，冪級数的系数 a_ν 属于 Δ (証明和上面一样). 不論系数 a_ν 如何选择，这个冪級数在 $\mathfrak{p}$-adic 賦值的意义之下永远是收斂的. 我們把算式(3)称为 $x-c$ 的形式冪級数.

习题. 1. 将 -1 和 $1/2$ 表成規范化的 3-adic 冪級数.

2. 設 f 为一整系数多項式. 方程 $f(\xi)=0$ 在域 Ω_p 中可解，当且仅当对每个自然数 n 同余式

$$f(\xi) \equiv 0 \pmod{p^n}$$

有一个有理解 ξ.

3. 方程

$$x^2 = -1, \quad x^2 = 3, \quad x^2 = 7$$

在域 Ω_3 中是否可解?

4. 設 $\mathfrak{p}$ 是多項式整环 $\Delta[x_1, x_2, \cdots, x_n]$ 中的理想 $(x_1, x_2, \cdots, x_n)$. 証明:对給定的 $f \not\equiv 0 \pmod{\mathfrak{p}}$ 同余式

$$fg \equiv 1 \pmod{\mathfrak{p}}$$

有一个解. 利用这一事实証明，域 $\Omega_\mathfrak{p}$ 由所有形式冪級数

$$h_0 + h_1 + h_2 + \cdots$$

的商組成，其中 h_k 是 $x_1, \cdots, x_n$ 的一个 k 次齐次式.

可能出现这样的情况，即域 $\mathbf{K}$ 的两个不同的賦值 φ 和 ψ 决定同一个完备扩域 Ω. 显然可見，这样一种情况出現，当且仅当 $\mathbf{K}$ 中的每叙列 $\{a_\nu\}$ 对 φ 来說为一零基本叙列时，对 ψ 来說也是零基本叙列，并且反之亦然. 在这样一种情况下，即当 $\lim\limits_{\nu\to\infty}\varphi(a_\nu)=0$ 和 $\lim\limits_{\nu\to\infty}\psi(a_\nu)=0$ 的意义完全相同时，我們說賦值 φ 和 ψ **等价**.

对于复数域的普通絕对値賦值 $\varphi(a)=|a|$，只要命 $\varphi(a)=|a|^\rho$，其中 ρ 是不大于 1 的任意正实数，就可作出无限多个和它等价的賦值. 条件 1. 至 3. 显然成立. 条件 4. 可由 $|a+b|\leqslant|a|+|b|$ 和不等式 $\varepsilon^\rho+\delta^\rho\leqslant(\varepsilon+\delta)^\rho$ 推出，这个不等式对任意两个实数 $\varepsilon\geqslant 0$, $\delta\geqslant 0$ 和任意 $0<\rho\leqslant 1$ 成立[1].

对有理数域的 p-adic 賦值 $\varphi_p(a)$ 来說，每个賦值 $\psi(a)=\varphi_p(a)^\sigma$ 都和它等价，其中 σ 表示任意一个固定的正数.

如果 φ 和 ψ 是域 $\mathbf{K}$ 的两个等价的賦值，則 ψ 是 φ 的一个冪，也就是說，存在一个固定的正数 s，使得对 $\mathbf{K}$ 中所有元素 a 有 $\psi(a)=\varphi(a)^s$.

証明. 如果 $\varphi(a)<\varphi(b)$ 則 $\psi(a)<\psi(b)$，并且反之亦然. 事实上，由 $\varphi(a)<\varphi(b)$ 可得 $\varphi(a/b)<1$，故当 $n\to\infty$ 时 $(a/b)^n$ 在賦值 φ 的意义之下收斂于零. 因此 $(a/b)^n$ 在賦值 ψ 的意义之下也收斂于零. 这就意味着 $\psi(a/b)<1$ 或 $\psi(a)<\psi(b)$. 現在設 p 是 $\mathbf{K}$ 中任意一个固定的元素，它使得 $\varphi(p)>1$. 这时也必有 $\psi(p)>1$. 設 a 是 $\mathbf{K}$ 中任意一个元素，且 $\varphi(a)=\varphi(p)^\delta$, $\psi(a)=\psi(p)^{\delta'}$. 我們要証明 $\delta=\delta'$. 設 n 和 m 是滿足条件 $n/m\leqslant\delta$ 的两个自然数，那末我們有

$$\varphi(p)^{n/m}\leqslant\varphi(p)^\delta=\varphi(a),\ 因而\ \varphi(p^n)\leqslant\varphi(a^m),$$

1) 參看 Hardy-Littlewood-Polya: Inequalities (不等式), Cambridge 1934, 第二章.

从这里即得

$$\psi(p^n) \leqslant \psi(a^m),\ \psi(p)^{n/m} \leqslant \psi(a) = \psi(p)^{\delta'},\ n/m < \delta'.$$

由于所有满足条件 $n/m \leqslant \delta$ 的分数 n/m 的上确界即 δ，故有 $\delta \leqslant \delta'$. 同样可知 $\delta' \leqslant \delta$，因而 $\delta = \delta'$. 注意 $\varepsilon = \dfrac{\log \psi(p)}{\log \varphi(p)}$ 是一个和 a 无关的正数，并且由于对所有的 a 都有 $\delta = \delta'$，故有

$$\log \psi(a) = \delta' \log \psi(p) = \delta \log \psi(p) = \delta\varepsilon \log \varphi(p) = \varepsilon \log \varphi(a),$$

因此

$$\psi(a) = \varphi(a)^{\varepsilon}.$$

設域 $\mathbf{K}$ 带有賦值 φ，域 $\mathbf{K}'$ 和 $\mathbf{K}$ 同构且带有賦值 ψ. 我們說 $\mathbf{K}$ 和 $\mathbf{K}'$ 之間的同构是**双方連續的**或**拓扑的**，如果 $\mathbf{K}$ 中的每个 φ-零叙列被这个同构映成 $\mathbf{K}'$ 中的一个 ψ-零叙列，并且反之亦然. 在这一情形下，域 $\mathbf{K}$ 和 $\mathbf{K}'$ 称为**連續同构的**. 在一个拓扑同构之下，收斂叙列和收斂叙列、基本叙列和基本叙列相互对应. 由此立即可以得出下面的結論：

連續同构的賦值域 $\mathbf{K}$ 和 $\mathbf{K}'$ 具有連續同构的完备扩域 $\Omega_{\mathbf{K}}$ 和 $\Omega_{\mathbf{K}'}$.

习题. 5. 証明：我們所知道的有理数域的各种賦值，即絕对值賦值和 p-adic 賦值之中，沒有两个賦值是等价的.

§ 76. 有理数域的賦值

下面这个由 Ostrowski 所首先証明的定理說明，我們所知道的有理数域的賦值，即絕对值賦值和 p-adic 賦值，本質上就是全部可能的賦值. 在这里我們仍旧假定值域就是实数域.

有理数域 Γ 的一个非不足道的賦值或者是 $\varphi(a) = |a|^{\rho}$，其中 $0 < \rho \leqslant 1$，因而和絕对值賦值等价；或者是 $\varphi(a) = \varphi_p(a)^{\sigma}$，其中 p 为固定素数，σ 为一固定正数，因而和一个 p-adic 賦值等

价.

証明. 对每个有理整数 n 有

$$\varphi(n) \leqslant |n|.$$

事实上我們有

$$\varphi(n) = \varphi(1 + 1 + \cdots + 1)$$
$$\leqslant \varphi(1) + \varphi(1) + \cdots + \varphi(1) \leqslant |n|.$$

現設 $a > 1$, $b > 1$ 是两个有理整数. 我們将 b^v 按 a 的冪展开

$$b^v = c_0 + c_1 a + \cdots + c_n a^n,$$
$$0 \leqslant c_v < a, \quad c_n \neq 0.$$

所出現的 a 的最高次冪 a^n 最多等于 b^v:

$$a^n \leqslant b^v,$$

即

$$n \leqslant v \frac{\log b}{\log a}.$$

命 $M = \max(1, \varphi(a))$. 由于

$$\varphi(b^v) \leqslant \varphi(c_0) + \varphi(c_1)\varphi(a) + \cdots + \varphi(c_n)\varphi(a)^n$$
$$< a(1 + \varphi(a) + \cdots + \varphi(a)^n) \leqslant a(n+1)M^n,$$

故有

$$\varphi(b)^v < a\left(\frac{\log b}{\log a} v + 1\right) M^{\frac{\log b}{\log a} v},$$

或

$$\left(\frac{\varphi(b)}{M^{\frac{\log b}{\log a}}}\right)^v < a \frac{\log b}{\log a} v + a.$$

根据 § 74 的引理,从这里可得

$$\varphi(b) \leqslant M^{\frac{\log b}{\log a}},$$

即

$$\varphi(b) \leqslant \max(1, \varphi(a)^{\frac{\log b}{\log a}}).$$

第一种情形. φ 为阿基米德賦値. 这时必有一整数 b, 使得 $\varphi(b)>1$. 如果对于任意另外某个整数 $a>1$ 有 $\varphi(a)\leqslant 1$, 则由刚才所証不等式将会得出矛盾 $\varphi(b)\leqslant 1$. 因此, 对所有整数 $a>1$ 有 $\varphi(a)>1$. 在这一情形上述不等式可写成

$$\varphi(b)\leqslant\varphi(a)^{\frac{\log b}{\log a}}$$

或

$$\varphi(b)^{\frac{1}{\log b}}\leqslant\varphi(a)^{\frac{1}{\log a}}.$$

另一方面, a 和 b 的地位是可以交换的, 因此也有

$$\varphi(a)^{\frac{1}{\log a}}\leqslant\varphi(b)^{\frac{1}{\log b}},$$

从而得

$$\varphi(a)^{\frac{1}{\log a}}=\varphi(b)^{\frac{1}{\log b}}.$$

如果 $\varphi(b)=b^{\rho}$, 那末由这个等式就可知 $\varphi(a)=a^{\rho}$, 因而对每个有理数 r

$$\varphi(r)=|r|^{\rho}.$$

由于 $\varphi(a)>1$, 故 $\rho>0$; 又由于

$$2^{\rho}=\varphi(2)=\varphi(1+1)\leqslant\varphi(1)+\varphi(1)=2,$$

故必有 $\rho\leqslant 1$.

第二种情形. φ 为非阿基米德賦値, 因而对所有整数 a, $\varphi(a)\leqslant 1$. 满足条件 $\varphi(a)<1$ 的整数 a 的全体显然是整数环中的一个理想. 这个理想是素的, 因为由 $\varphi(ab)=\varphi(a)\varphi(b)<1$ 必有 $\varphi(a)<1$ 或 $\varphi(b)<1$. 我們知道, 整数环中每个理想都是主理想, 特别每个素理想都由一个素数生成. 因此, 满足条件 $\varphi(a)<1$ 的整数 a 恰恰就是某一素数 p 的所有倍数. 每个有理数 r 都可以表成 $r=\frac{z}{n}p^{\rho}$ 的形式, 其中 n 和 z 都不能被 p 整除. 由于 $\varphi(z)=\varphi(n)=1$, 故有 $\varphi(r)=\varphi(p)^{\rho}=p^{-\rho\sigma}=\varphi_p(r)^{\sigma}$,

这里 $\sigma = -\frac{\log \varphi(p)}{\log p}$ 是一个固定的数，并且由于 $\varphi(p) < 1$，这个数是正的。

有理数域 Γ 的賦值完全确定之后，我們可以进一步考虑代数扩域和超越扩域。先从代数扩域入手。

这里我們主要限于考虑非阿基米德賦値；阿基米德賦值的意义比較小。事实上，Ostrowski 曾經証明，**任何一个阿基米德賦值域 K 都和一个由复数組成而以普通絕对值賦值的域連續同构**。关于这个定理的証明可以参看 Ostrowski 的原作[1]。

因此，我們为自己提出如下的一个綱領：假設已經給定了域 $\mathbf{K}$ 的一个(非阿基米德)賦值 φ。我們考虑 $\mathbf{K}$ 的一个代数扩域 Λ，并提出这样的問題：域 $\mathbf{K}$ 的賦值 φ 能不能、且有多少种方式可以开拓成域 Λ 的賦值 Φ。

在 § 77 中我們假定 $\mathbf{K}$ 是一个完备的賦值域。在 § 78 中，我們通过嵌入的办法将非完备賦値域的情形归結为完备的情形。在 § 79 中我們利用所得到的結果来确定一个任意的代数数域的所有阿基米德与非阿基米德賦值。在 § 80 到 82 中类似地考虑了代数函数域的賦值。

习題. 設 $\varphi_0(a) = |a|$ 而 $\varphi_p(a)$ 是 p-adic 賦值，則对每个固定的元素 a 所有这些值的积等于 1。

§ 77. 代数扩域的賦值：完备情形

設域 $\mathbf{K}$ 对指数賦值 $w(a) = \log \varphi(a)$ 来説是完备的，卽在 $\mathbf{K}$

---

1) Ostrowski, A.: Über einige Lösungen der Funktionalgleichung $\varphi(x)\varphi(y) = \varphi(xy)$ (論函数方程 $\varphi(x)\varphi(y) = \varphi(xy)$ 的某些解), *Acta Math.*, **41** (1918), 271—284. Ostrowski 发表在 *Math. Z.*, **39** (1934), 296—404 頁的另一长篇論文乃是下文的基础。

中 Cauchy 收斂准則成立。 我們要研究怎样把这个指数賦值开拓到 **K** 的代数扩域 Λ 上去。

让我們再提醒一次，滿足条件 $w(a) \geqslant 0$ 的元素 a 称为整元素，它們組成一个环；滿足条件 $w(a) > 0$ 的元素 a 組成这个环中的一个素理想 $\mathfrak{p}$。

由 Hensel 所建立的、完备域中的一个可約性准則，乃是下面的研究的基础。

設指数賦值域中多項式

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

的系数当中 a_ν 的指数最小，那末多項式

$$\frac{a_n}{a_\nu} x^n + \frac{a_{n-1}}{a_\nu} x^{n-1} + \cdots + \frac{a_0}{a_\nu}$$

的系数全是整的，并且不全属于 $\mathfrak{p}$。这样一个多項式称为一个本原多項式。

Hensel 引理. 設 **K** 对指数賦值 w 是完备的。$f(x)$ 是以 **K** 中整元素为系数的一个本原多項式。 如果 $g_0(x)$ 和 $h_0(x)$ 是以 **K** 中整元素为系数的多項式，并且条件

$$f(x) \equiv g_0(x) h_0(x) \pmod{\mathfrak{p}}$$

成立，那末可以找到两个以 **K** 中整元素为系数的多項式 $g(x)$ 和 $h(x)$，使得

$$f(x) = g(x) h(x),$$
$$g(x) \equiv g_0(x) \pmod{\mathfrak{p}},$$
$$h(x) \equiv h_0(x) \pmod{\mathfrak{p}},$$

这里我們假定 $g_0(x)$ 和 $h_0(x)$ 是模 $\mathfrak{p}$ 互素的。 除此之外，$g(x)$ 和 $h(x)$ 还可以这样选择，使得 $g(x)$ 的次数等于 $g_0(x)$ 模 $\mathfrak{p}$ 的次数。

証明. 由于我們可以从 $g_0(x)$ 和 $h_0(x)$ 中去掉能被 $\mathfrak{p}$ 整除

的系数，而不影响整个引理的条件与結論，故可事先假定 $g_0(x)$ 是一个 r 次多項式，且 $g_0(x)$ 和 $h_0(x)$ 的首項系数都是可逆元素．此外，当我們把 $g_0(x)$ 换成 $\frac{1}{a}g_0(x)$，$h_0(x)$ 换成 $ah_0(x)$ 时，也不会产生任何影响．因此可以假定 $g_0(x)$ 是一个規范化的 r 次多項式，即其首項系数等于1：$g(x)=x^r+\cdots$．这样一来，如果 $h_0(x)$ 的首項系数为 b，次数为 s，則乘积 $g_0(x)h_0(x)$ 的首項系数等于 b，而其次数等于 $r+s\leqslant n$．現在我們要作出多項式 $g(x)$ 和 $h(x)$，使得 $g(x)$ 是一个 r 次的規范化多項式，从而 $h(x)$ 是一个 $n-r$ 次多項式．

根据我們的假設，多項式 $f(x)-g_0(x)h_0(x)$ 的系数全都具有正的指数；設其中最小者为 $\delta_1>0$．如果 $\delta_1=\infty$，則 $f(x)=g_0(x)h_0(x)$，那就沒什么要証明的了．

由于 $g_0(x)$ 和 $h_0(x)$ 模 $\mathfrak{p}$ 互素，故可找到两个以 $\mathbf{K}$ 中整元素为系数的多項式 $l(x)$ 和 $m(x)$，使得

$$l(x)g_0(x)+m(x)h_0(x)\equiv 1\pmod{\mathfrak{p}}.$$

設多項式

$$l(x)g_0(x)+m(x)h_0(x)-1$$

的系数当中最小的指数为 $\delta_2>0$，并設 δ_1，δ_2 二数中較小者为 ε，最后設 π 是滿足条件 $w(\pi)=\varepsilon$ 的元素，則有

$$f(x)\equiv g_0(x)h_0(x)\pmod{\pi},\tag{1}$$

$$l(x)g_0(x)+m(x)h_0(x)\equiv 1\pmod{\pi}.\tag{2}$$

我們所要造的多項式 $g(x)$ 是一串 r 次多項式 $g_\nu(x)$ 的极限，其中头一个多項式是 $g_0(x)$；$h(x)$ 是一串次数 $\leqslant n-r$ 的多項式 $h_\nu(x)$ 的极限，其中头一个多項式是 $h_0(x)$．假設 $g_\nu(x)$ 和 $h_\nu(x)$ 已經造出，且滿足条件

$$f(x)\equiv g_\nu(x)h_\nu(x)\pmod{\pi^{\nu+1}},\tag{3}$$

(4) $$g_\nu(x) \equiv g_0(x) \pmod{\pi},$$

(5) $$h_\nu(x) \equiv h_0(x) \pmod{\pi},$$

而 $g_\nu(x)=x^r+\cdots$ 的首項系数为 1. 为了造出 $g_{\nu+1}(x)$ 和 $h_{\nu+1}(x)$，我們先試命

(6) $$g_{\nu+1}(x) = g_\nu(x) + \pi^{\nu+1}u(x)$$

(7) $$h_{\nu+1}(x) = h_\nu(x) + \pi^{\nu+1}v(x).$$

这时就有

$$\begin{cases} g_{\nu+1}(x)h_{\nu+1}(x) - f(x) = g_\nu(x)h_\nu(x) - f(x) + \\ \quad + \pi^{\nu+1}\{g_\nu(x)v(x) + h_\nu(x)u(x)\} + \pi^{2\nu+2}u(x)v(x). \end{cases}$$

根据 (3) 可命

$$f(x) - g_\nu(x)h_\nu(x) = \pi^{\nu+1}p(x),$$

这样便得

$$\begin{cases} g_{\nu+1}(x)h_{\nu+1}(x) - f(x) \equiv \pi^{\nu+1}\{g_\nu(x)v(x) + \\ \quad + h_\nu(x)u(x) - p(x)\} \pmod{\pi^{\nu+2}}. \end{cases}$$

为了使得左端能被 $\pi^{\nu+2}$ 整除，只須满足同余式

(8) $$g_\nu(x)v(x) + h_\nu(x)u(x) \equiv p(x) \pmod{\pi}$$

即可.

为了达到这一目的，我們将同余式 (2) 乘以 $p(x)$

(9) $$p(x)l(x)g_0(x) + p(x)m(x)h_0(x) \equiv p(x) \pmod{\pi},$$

以 $g_0(x)$ 除 $p(x)m(x)$，其剩余 $u(x)$ 为一次数 $< r$ 的多項式：

(10) $$p(x)m(x) = q(x)g_0(x) + u(x),$$

将(10)代入(9)得

$$\{p(x)l(x)+q(x)h_0(x)\}g_0(x)+u(x)h_0(x) \equiv p(x) \pmod{\pi},$$

将花括号中所有能被 π 整除的系数都换成 0，就得到

(11) $$v(x)g_0(x) + u(x)h_0(x) \equiv p(x) \pmod{\pi}.$$

由于(4)和(5)，从(11)即得所要求的同余式(8). 其次，$u(x)$ 的次

数 $< r$，因此，由(6)可知 $g_{\nu+1}(x)$ 和 $g_\nu(x)$ 有相同的次数和首項系数．現在只要証明 $v(x)$ 的次数 $\leqslant n-r$ 就行了．假如不是这样的話，(11) 的第一項中将会出現一个次数 $> n$ 的最高次項，而其余各項的次数都不大于 n．因此，根据 (11)，这个最高次項的系数能被 π 整除，从而 $v(x)$ 的首項系数能被 π 整除．另一方面，由于 $v(x)$ 的系数当中能被 π 整除的均已去掉，故知 $v(x)$ 的次数 $\leqslant n-r$．

在上面我們已經看到，由同余式 (8) 即有

$$f(x) \equiv g_{\nu+1}(x)h_{\nu+1}(x) \pmod{\pi^{\nu+2}}. \tag{12}$$

由 (6) 可以看出，多項式 $g_{\nu+1}(x) - g_\nu(x)$ 的系数能被 $\pi^{\nu+1}$ 整除．因此，当 $\nu \to \infty$ 时，这些系数的极限是零．根据 Cauchy 收斂准則可知，当 $\nu \to \infty$ 时 $g_\nu(x)$ 收斂于一个多項式

$$g(x) = x^r + \cdots.$$

同样，当 $\nu \to \infty$ 时，$h_\nu(x)$ 收斂于一个多項式 $h(x)$．最后，在 (3) 中取极限即得

$$f(x) = g(x)h(x),$$

而由 (4) 和 (5) 取极限可得

$$g(x) \equiv g_0(x) \pmod{\mathfrak{p}},$$

$$h(x) \equiv h_0(x) \pmod{\mathfrak{p}}.$$

一个簡单的推論：

如果

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

是 **K** 中的不可約多項式，則

$$\min(w(a_0), w(a_1), \cdots, w(a_n)) = \min(w(a_0), w(a_n)).$$

为了証明这一点，我們假定 $f(x)$ 是本原的．这时 $\min(w(a_0), \cdots, w(a_n))$ 等于零．假如 $w(a_0)$ 和 $w(a_n)$ 都大于零，那末一定

有一个 r, $0 < r < n$, 使得 $w(a_r) = 0$, 而当 $\nu = r+1, \cdots, n$ 时, $w(a_\nu) > 0$. 这样一来,便有

$$f(x) \equiv (a_0 + a_1 x + \cdots + a_r x^r) \cdot 1 \pmod{\mathfrak{p}}$$
$$0 < r < n.$$

因此, 根据 Hensel 引理, $f(x)$ 可分解一个 r 次因子和一个 $n-r$ 次因子.

习題. 1. 如果一个多項式 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ 以 $\mathbf{K}$ 中整元素为系数, 并且模 $\mathfrak{p}$ 不可約, 那末 $f(x)$ 在完备域 $\Omega_{\mathbf{K}}$ 中也是不可約的.

2. 如果在 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ 中所有系数 $a_{n-1}, \cdots, a_0$ 都属于 $\mathfrak{p}$, 并且 a_0 不能表成 $\mathfrak{p}$ 中两个元素的积, 則 $f(x)$ 是不可約的 (Eisenstein 不可約准則的推广).

3. 試研究有理数域中的不可約多項式

$$x^2 + 1, \quad x^2 + 2, \quad x^2 - 3$$

在 3-adic 数域中的因子分解問題[利用习題 1, Hensel 引理和习題 2].

最后这个定理的一个最重要的应用, 就是証明完备指数賦值 w 可以开拓到代数扩域上去.

設域 $\mathbf{K}$ 对指数賦值 w 来說是完备的, Λ 是 $\mathbf{K}$ 的一个代数扩域, 那末可以作出域 Λ 的一个指数賦值 W, 使得它在 $\mathbf{K}$ 上和 w 一致.

証明. 1. 設 ξ 是 Λ 中的一个元素, 而

$$\xi^n + a_{n-1}\xi^{n-1} + \cdots + a_0 = 0$$

是 ξ 所满足的系数属于 $\mathbf{K}$ 的不可約方程. 我們断言

$$W(\xi) = \frac{1}{n} w(a_0)$$

是 Λ 的一个賦值(这个賦值在 $\mathbf{K}$ 上显然和 w 一致). 为了对 Λ 中的两个元素 ξ 和 η 証明关系式

$$W(\xi\eta) = W(\xi) + W(\eta)$$
$$W(\xi + \eta) \geqslant \min(W(\xi), W(\eta)),$$

我們考虑子域 $\Lambda_0 = \mathbf{K}(\xi, \eta)$，这个子域在 $\mathbf{K}$ 上有有限次数 t. 我們在这个子域中作 ξ 的范数. 根据 § 44，有

$$N(\xi) = (-1)^t a_0^r, \quad r = \frac{t}{n},$$

因此

$$w(N(\xi)) = w(a_0^r) = r w(a_0).$$

$$W(\xi) = \frac{1}{n} w(a_0) = \frac{1}{t} w(N(\xi)).$$

由于 $N(\xi\eta) = N(\xi)N(\eta)$，故从这里立即得出

$$W(\xi\eta) = W(\xi) + W(\eta).$$

証明不等式 $W(\xi + \eta) \geqslant \min(W(\xi), W(\eta))$ 时，由于

$$W(\xi + \eta) = W(\eta) + W\left(1 + \frac{\xi}{\eta}\right)$$

和

$$\min(W(\xi), W(\eta)) = W(\eta) + \min\left(W\left(\frac{\xi}{\eta}\right), 0\right),$$

我們可以仅限于 $\eta = 1$ 的情形.

另一方面，$\xi + 1$ 所滿足的不可約方程是

$$(\xi + 1)^n + \cdots + (a_0 - a_1 + a_2 - \cdots + \\ + (-1)^{n-1} a_{n-1} + (-1)^n) = 0,$$

因而根据前面的定理的确有

$$W(\xi + 1) = \frac{1}{n} w(a_0 - a_1 + \cdots) \geqslant$$

$$\geqslant \frac{1}{n} \min(w(a_0), w(a_1), \cdots, w(a_{n-1}), w(1)) =$$

$$= \frac{1}{n} \min(w(a_0), w(1)) = \min(W(\xi), 0).$$

由指数賦值 $w(a)$, $W(\xi)$ 过渡到普通賦值

$$\varphi(a) = e^{-w(a)}, \quad \Phi(\xi) = e^{-W(\xi)}$$

时，扩张 Λ 的赋值由公式

$$\Phi(\xi) = \sqrt[n]{\varphi(a_0)}$$

确定；当 Λ 对 $\mathbf{K}$ 的次数为有限数 t 时，由公式

$$\Phi(\xi) = \sqrt[t]{\varphi(N_\Lambda(\xi))}$$

确定.

我們指出，完全同样的公式在阿基米德赋值的情形也成立. 唯一的非不足道的情况就是 $\mathbf{K}$ 为实数域而 Λ 为复数域的情形. $\mathbf{K}$ 的賦値

$$\varphi(\xi) = |\xi|^\rho$$

显然可以开拓成 Λ 的賦値

$$\Phi(\xi) = |\xi|^\rho.$$

另一方面，对 $\xi = a + bi$ 有

$$|\xi| = \sqrt{a^2 + b^2} = \sqrt{N(\xi)} = \sqrt{|N(\xi)|},$$

故

$$\Phi(\xi) = |\xi|^\rho = \sqrt{\varphi(N(\xi))}.$$

由于这样一个情况，从現在起我們又把阿基米德賦値和非阿基米德賦値放在一起考慮，并将 $\mathbf{K}$ 或者理解为一个完备的非阿基米德賦値域，或者理解为实数或复数域，其中的賦値为絕对值賦値 $\varphi(a) = |a|^\rho$.

設域 Λ 对域 $\mathbf{K}$ 的次数是有限的，而 $u_1, u_2, \cdots, u_n$ 是 $\Lambda/\mathbf{K}$ 的一个基，并設 $\mathbf{K}$ 对賦値 φ 来說是完备的. 如果 Φ 是 Λ 的一个賦値，它在 $\mathbf{K}$ 上和 φ 相一致，那末 Λ 中的一个叙列

$$c_\nu = a_1^{(\nu)}u_1 + \cdots + a_n^{(\nu)}u_n, \quad \nu = 1, 2, 3, \cdots,$$

对 Φ 来說是一个基本叙列，当且仅当 n 个叙列 $\{a_i^{(\nu)}\}$ 对 φ 来說是基本叙列.

由于叙列 $a_i^{(\nu)}$ 在 $\mathbf{K}$ 中分别收斂于极限 a_i，故知 Λ 对 Φ 来說是

完备的.

証明. 叙列 $\{a_i^{(\nu)}\}$ 的收斂性可以用完全归納法証明如下:如果叙列 c_ν 具有形式

$$c_\nu = a_1^{(\nu)} u_1,$$

那末只要 $\{c_\nu\}$ 是一个基本叙列, 叙列 $\{a_1^{(\nu)}\}$ 也自然是一个基本叙列. 現在假設上述断言对所有形为

$$c_\nu = \sum_{i=1}^{m-1} a_i^{(\nu)} u_i$$

的叙列已經証明,并設已經給定了一基本叙列

$$c_\nu = \sum_{i=1}^{m} a_i^{(\nu)} u_i.$$

如果叙列 $\{a_m^{(\nu)}\}$ 收斂,則 $\{c_\nu - a_m^{(\nu)} u_m\}$ 也是基本叙列,因而根据归納假設,叙列 $\{a_i^{(\nu)}\}$, $i < m$, 收斂. 現在假設 $\{a_m^{(\nu)}\}$ 不收斂,那末我們可以选择一个自然数叙列 $n_1, n_2, n_3, \cdots$, 使得对所有的 ν 有 $\varphi(a_m^{(\nu)} - a_m^{(\nu+n_\nu)}) > \varepsilon$,其中 ε 为一固定正数. 叙列

$$d_\nu = \frac{c_\nu - c_{\nu+n_\nu}}{a_m^{\nu} - a_m^{(\nu+n_\nu)}} = \sum_{i=1}^{m-1} \frac{a_i^{(\nu)} - a_i^{(\nu+n_\nu)}}{a_m^{(\nu)} - a_m^{(\nu+n_\nu)}} u_i + u_m$$
$$= \sum_{i=1}^{m-1} b_i^{(\nu)} u_i + u_m$$

必趋向零. 事实上, 由于 $\{c_\nu\}$ 是一个基本叙列,分子的叙列必趋向零. 我們有

$$d_\nu - u_m = \sum_{i=1}^{m-1} b_i^{(\nu)} u_i.$$

根据归納假設,叙列 $\{b_i^{(\nu)}\}$ 收斂于极限 b_i, 并有

$$-u_m = \sum_{i=1}^{m-1} b_i u_i,$$

然而这是与 $u_1, \cdots, u_n$ 为 $\Lambda/\mathbf{K}$ 的基这一事实相违背的.

用完全同样的办法可以証明，叙列 $\{c_\nu\}$ 为零叙列，当且仅当叙列 $\{a_i^{(\nu)}\}(i=1, \cdots, n)$ 为零叙列.

在这样一点注意的基础之上可以証明下面的唯一性定理:

完备域 $\mathbf{K}$ 的賦值 φ 到代数扩张 Λ 上的开拓 Φ 是唯一地确定的，且有

$$\Phi(\xi)=\sqrt[n]{\varphi(N(\xi))},$$

其中的范数 $N(\xi)$ 是在域 $\mathbf{K}(\xi)$ 中作出的，而 n 是 $\mathbf{K}(\xi)$ 对 $\mathbf{K}$ 的次数.

証明. 只要考虑一个固定的元素 ξ 及与之相应的域 $\mathbf{K}(\xi)$ 就行了，所考虑的范数都是指的在这个域中作出的范数. 如果这个域中一个叙列 $\{c_\nu\}$ 趋向零（在 Φ 的意义下），那末，根据上面所述，当我們将 c_ν 通过 $\mathbf{K}(\xi)$ 的基元素 $u_1, \cdots, u_n$ 綫性地表出时，表示式中的系数 $a_i^{(\nu)}$ 也将趋向零. c_ν 的范数是这些系数的齐次多項式，因此这些范数也趋向零. 现在假設 $\Phi(\xi)^n<\varphi(N(\xi))$ 或 $\Phi(\xi)^n>\varphi(N(\xi))$. 我們分别考虑

$$\eta=\frac{\xi^n}{N(\xi)}$$

和

$$\eta=\frac{N(\xi)}{\xi^n}.$$

在两种情形下都有 $N(\eta)=1$ 和 $\Phi(\eta)<1$. 因此 $\lim \eta^\nu=0$，从而 $\lim N(\eta^\nu)=0$. 然而这是和 $N(\eta^\nu)=N(\eta)^\nu=1$ 这一事实相违背的.

习題. 4. 完备賦值域 $\mathbf{K}$ 的两个賦值代数扩域 Λ 和 Λ' 之間的一个同构，如果它使得 $\mathbf{K}$ 的元素不动的話，必将 Λ 的賦值变为 Λ' 的賦值.

5. 复数域只有一个賦值 Φ，它在实数域上和 $\varphi(a)=|a|^\rho$ 相一致. 这个賦值就是 $\Phi(a)=|a|^\rho$.

§78. 代数扩域的賦值：一般情形

設 $\mathbf{K}$ 是一个任意的賦值域，Λ 是 $\mathbf{K}$ 的一个代数扩域．我們問：能不能和有多少种方式可以将 $\mathbf{K}$ 中給定的賦值 φ 开拓成 Λ 的一个賦值．

为了表述簡单起見，我們先只限于考虑单純扩域 $\Lambda=\mathbf{K}(\vartheta)$ 的情形，并設 ϑ 是 $\mathbf{K}[x]$ 中的不可約多項式 $F(x)$ 的零点．

我們先将域 $\mathbf{K}$ 扩张成完备賦值域 Ω，这个域可以按照 §75 中的方法作出，然后再作多項式 $F(x)$ 在 Ω 之上的分裂域 Σ．根据 §77，Ω 的賦值 φ 可唯一开拓到 Σ 上去．

所謂域 Λ 到域 Σ 之內的一个**嵌入**，指的就是一个同构 σ，它将 $\Lambda=\mathbf{K}(\vartheta)$ 映成 Σ 的一个子域 $\mathbf{K}(\vartheta')$，而使得基域 $\mathbf{K}$ 的元素不动．同构 σ 将 ϑ 映成 $F(x)$ 的一个零点 ϑ'，并且 σ 完全由 ϑ' 确定．我們断言：

Λ 到 Σ 之內的每个嵌入决定 Λ 的一个賦值． 事实上，Λ' 作为 Σ 的一个子域来看自然是賦值的，而同构 σ^{-1} 将 Λ' 的賦值轉移为 Λ 的賦值．显然，这样得到的 Λ 的賦值乃是 $\mathbf{K}$ 的賦值 φ 的一个开拓．

我們断言：

Λ 的每一个賦值，如果它是 $\mathbf{K}$ 的賦值 φ 的开拓的話，都可通过上述方式由 Λ 到 Σ 之內的嵌入得出．

証明．　我們作出 Λ 的完备扩张．这个完备扩张包含着 $\mathbf{K}$ 的完备扩张 Ω，并且包含着 ϑ，因而包含着域 $\Omega(\vartheta)$．另一方面，$\Omega(\vartheta)$ 可以扩张成多項式 F 的一个和 Σ 同构的分裂域．这一同构将 $\Omega(\vartheta)$ 映成 Σ 的一个子域 $\Omega(\vartheta')$，而使得 Ω 中的元素不动，因而将 $\Omega(\vartheta)$ 的賦值轉移成 $\Omega(\vartheta')$ 中的唯一可能的賦值．

对上面的証明来說，单純扩域的限制是完全无关紧要的．如果不是考虑一个代数量 ϑ，而是有限多个代数量 $\zeta_1, \zeta_2, \cdots, \zeta_t$，且这些代数量分别是 $\mathbf{K}[x]$ 中的多项式 $g_1, \cdots, g_t$ 的零点，那末我們可取乘积 $g_1 \cdots g_t$ 的分裂域作为 Σ，然后和上面一样地进行推論．如果 Λ 是 $\mathbf{K}$ 的一个无限代数扩域，則可取 Ω 的代数封閉扩域作为 Σ，証明仍旧和上面一样．

現在让我們仍旧返回来考虑单純扩张的情形，并在 $\Omega[x]$ 中将定义多项式 $F(x)$ 分解成不可約因子

$$F(x) = F_1(x)F_2(x)\cdots F_s(x).$$

$\mathbf{K}(\vartheta)$ 的每个同构 σ 将 ϑ 映成某一多项式 $F_\nu(x)$ 的一个零点．相应于每个 $F_\nu(x)$ 都有一个扩域 $\Omega(\vartheta_\nu)$，其中 ϑ_ν 是 $F_\nu(x)$ 的任意一个零点：究竟是哪一个零点，那是沒有差别的，因为一个不可約多项式的所有零点都是相互共軛的．

如果一个同构 σ 将元素 ϑ 映成 ϑ_ν，而使得 $\mathbf{K}$ 中的元素不动，那末它就将每个多项式 $g(\vartheta)$ 映 $g(\vartheta_\nu)$，故 σ 由 ϑ_ν 所完全决定．因此，$\Lambda = \mathbf{K}(\vartheta)$ 到 Σ 之內的一切可能的嵌入由对应

$$\vartheta \to \vartheta_\nu \quad (\nu = 1, \cdots, s)$$

决定．这样一来，Λ 的賦值也就随之决定：要想得到任意某个元素 $\eta = g(\vartheta)$ 的值，先作出它的第 ν-个共軛元素

$$\eta_\nu = g(\vartheta_\nu),$$

然后根据 § 77 計算这个共軛元素的值

$$\Phi(\eta_\nu) = \sqrt[n_\nu]{\varphi(N(\eta_\nu))},$$

其中 n_ν 是多项式 F_ν 的次数，而范数 $N(\eta_\nu)$ 則是在域 $\Omega(\vartheta_\nu)$ 中作出的．因此

賦值 φ 的开拓的个数恰等于多项式 $F(x)$ 在 $\Omega[x]$ 中的不可約因子的个数．

§79. 代数数域的赋值

前一节中的一般理論在代数数域的例子上得到了非常出色的說明.

設 $\Lambda = \Gamma(\vartheta)$ 是一个代数数域，即将一个本原元素 ϑ 添加于有理数域 Γ 而得到的一个有限扩域，并設 $F(x)$ 是以 ϑ 为零点的規范化的不可約多項式.

如果将等价的賦值看作相同，則基域 Γ 有一个唯一的阿基米德賦值 $\varphi(a) = |a|$，此外，对每个素数 p 有一个非阿基米德賦值，即 p-adic 賦值：

$$\varphi_p(a) = p^{-m},$$

其中 m 是有理数 a 的因子分解中 p 的指数.

和阿基米德賦值相当的完备扩张就是实数域 $\mathbf{P}$. 再添加一个 i，这个域就成为代数封閉的，多項式 $F(x)$ 分解成一次因子：

$$F(x) = (x - \vartheta_1)(x - \vartheta_2)\cdots(x - \vartheta_n)$$

为了得出实的分解，我們将两个相互共軛的复因子合并成一个实的二次式：

$$(x - a - bi)(x - a + bi) = (x - a)^2 + b^2.$$

設 r_1 是实根的个数，r_2 是共軛复根对的个数，則 $F(x)$ 分解成 $r_1 + r_2$ 个实不可約因子.

相应于每个这样的因子有 Λ 的一个賦值，只要用一个将 ϑ 映成实或复根 ϑ_ν 的同构将 Λ 嵌入到实或复数域中去，就可得出这个相应的賦值来，但在两个共軛的复根中每次只要取其中一个就行了. 这个同构将 ϑ 的每个函数

$$\eta = g(\vartheta) = c_0 + c_1\vartheta + \cdots + c_{n-1}\vartheta^{n-1}$$

映成 ϑ_ν 的相应的函数

$$\eta_\nu = g(\vartheta_\nu) = c_0 + c_1\vartheta_\nu + \cdots + c_{n-1}\vartheta_\nu^{n-1}.$$

因此，相应的阿基米德賦値是

$$\varphi(\eta) = |\eta_\nu|.$$

这就是說：η 的 $r_1 + r_2$ 个阿基米德賦値由与 η 共軛的实数与复数 η_ν 的絕对値給出，这里从两个共軛复数中只取其一。

代数数域的 $r_1 + r_2$ 个阿基米德賦値和域中的可逆元素有着十分密切的关系。参看 B. L. van der Waerden, *Abh. Math. Sem. Hamburg*, **6**(1928), 259.

p-adic 賦値的研究可以完全类似地进行．相应于 Γ 的賦値 φ_p 的完备域卽 p-adic 数域 Ω_p．我們在 Ω_p 中将 $F(x)$ 分解成不可約因子：

$$F(x) = F_1(x)F_2(x)\cdots F_s(x). \tag{1}$$

对每个不可約多項式 F_ν，我們将它的一个零点 ϑ_ν 添加到 Ω_p 上，并作出相应的同构将 $\eta = g(\vartheta)$ 映成 $\eta_\nu = g(\vartheta_\nu)$ $(\nu = 1, \cdots, s)$．由这一同构卽得出賦値

$$\varphi_\nu(\eta) = \Phi_p(\eta_\nu) = \sqrt[n_\nu]{\varphi_p(N_\nu(\eta_\nu))}. \tag{2}$$

这里的范数 $N_\nu(\eta_\nu)$ 就是 η_ν 的全部共軛元素的乘积，只要在 $\eta_\nu = g(\vartheta_\nu)$ 中将 ϑ_ν 依次换成多項式 $F_\nu(x)$ 的全部根，就可以得出这些共軛元素来．設 $F_\nu(x)$ 的根是 $\vartheta_{\nu 1}, \vartheta_{\nu 2}, \cdots$，則

$$N_\nu(\eta_\nu) = g(\vartheta_{\nu 1}) \cdot g(\vartheta_{\nu 2}) \cdots \tag{3}$$

是根 $\vartheta_{\nu 1}, \vartheta_{\nu 2}, \cdots$ 的一个对称函数，因而可由 F_ν 的系数表出．这样，只要知道了分解式 (1)，我們就可以利用公式 (2) 找出所有的賦値 $\varphi(x)$ 来．

可是怎样才能找出整系数多項式 $F(x)$ 在 p-adic 数域 Ω_p 中的因子分解呢？

这里一个重要的輔助工具就是 Hensel 引理(§ 77)：如果 $F(x)$

模 p 可以分解成两个互素的因子 $G_0(x)\cdot H_0(x)$，那末 $F(x)$ 在完备域 Ω_p 中也可以分解成两个因子 $G(x)\cdot H(x)$，其中 $G(x)$ 的次数等于 $G_0(x)$ 模 p 的次数．Hensel 引理的証明同时还給了我們一工具，通过"逐次逼近"（第一步模 p，第二步模 p^2 等等）的办法来計算因子 G 和 H．

另一方面，如果 $F(x)$ 模 p 不可約，则 $F(x)$ 在 p-adic 数域 Ω_p 中也是不可約的（§ 77，习題 1）．

最困难的情形就是在 $F(x)$ 的模 p 因子分解中出現重因子．在这一情形下 Eisenstein 的不可約准则（§ 77，习題 2）往往很有帮助．

例． 試定出二次域 $\Lambda = \Gamma(\sqrt{5})$ 的全部賦值．

以 $\vartheta = \sqrt{5}$ 为零点的定义多项式是

$$F(x) = x^2 - 5.$$

在实数域中 $F(x)$ 分解成两个实的一次因子

$$F(x) = (x - \sqrt{5})(x + \sqrt{5}).$$

因此，当我們把 ϑ 映成 $-\sqrt{5}$ 或 $\sqrt{5}$ 时，可能得到两种不同的嵌入．設

$$\eta = a + b\vartheta$$

为任意的域元素，则相应的賦值是

$$\varphi_0(\eta) = |a + b\sqrt{5}| \tag{4}$$

和

$$\varphi_1(\eta) = |a - b\sqrt{5}|. \tag{5}$$

这样我們就把两个阿基米德賦值找出来了．現在让我們来考虑 p-adic 賦值．

$F(x)$ 的判别式等于 20．我們暂把能整除判别式的两个素数 2 和 5 除外．

对所有其余的素数来說，$F(x)$ 模 p 无重因子．因此只可能

出現两种情况：或者 $F(x)$ 模 p 不可約，或者 $F(x)$ 模 p 分解成两个一次因子。如果一个因子是 $x-c$，则另一因子是 $x+c$，因为 x^2-5 的两个零点之和必等于零。因此，在第二种情形下我們有

(6) $$x^2-5\equiv(x-c)(x+c)\pmod p,$$

$$5\equiv c^2\pmod p.$$

这就是說，存在一个整数 c，其平方模 p 同余于 5。我們也說，5 是一个模 p **二次剩余**。

反之，如果 $c^2\equiv 5(p)$，则分解式 (6) 成立。因此，**如果 5 不是一个模 p 二次剩余，则 x^2-5 模 p 不可約；如果 5 是二次剩余，则 x^2-5 模 p 分解成两个一次因子。**

从初等数論中的二次互反律可知，对所有素数 $p\equiv\pm 1\ (5)$ 来說 5 是二次剩余，而对所有奇素数 $p\equiv\pm 2\ (5)$ 来說，5 不是二次剩余。

在第一种情形下 $F(x)$ 也是 p-adic 不可約的；在第二种情形下，根据 Hensel 引理，$F(x)$ 在 Ω_p 中可分解成两个一次因子。

根据前面所述，在第一种情形下相应于素数 p 只有一个賦值

$$\varphi(\eta)=\sqrt{\varphi_p(N(\eta))}.$$

再一次命

$$\eta=a+b\vartheta=a+b\sqrt{5},$$

则有

$$N(\eta)=(a+b\sqrt{5})(a-b\sqrt{5})=a^2-5b^2$$

因此，对所有使得 5 不是二次剩余的素数 p 来說

(7) $$\varphi(\eta)=\sqrt{\varphi_p(a^2-5b^2)}$$

素数 3 和 7 就属于这一类。

以 $p=11$ 为模时，5 是一个二次剩余，因为我們有

$$4^2\equiv 5\pmod{11}.$$

对于这样的素数，根据 Hensel 引理，我們有 p-adic 分解

(8) $$x^2 - 5 = (x - \gamma)(x + \gamma).$$

p-adic 数 γ 可以用下面的办法求出：解同余式

$$c^2 \equiv 5,$$

先对模 p 求解，再对模 p^2 求解，余此类推. 每次都可以得到两个解 c 和 $-c$. 这样，我們就得到以 $p, p^2, \cdots$ 为模的两个同余类叙列，在每个叙列中每个同余类包含在前一个同余类之內. 其中一个叙列决定 γ，另一叙列决定 $-\gamma$.

举例来說，为了解同余式

$$c^2 \equiv 5 \pmod{11^2},$$

我們命

$$c = 4 + 11x$$

$$c^2 \equiv 16 + 88x \pmod{11^2}$$

$$16 + 88x \equiv 5 \pmod{11^2}$$

$$88x \equiv -11 \pmod{11^2}$$

$$8x \equiv -1 \pmod{11}$$

$$x = 4$$

$$c = 4 + 11x = 48.$$

最后，为了得到 Γ 的 p-adic 賦值 φ_p 的两个开拓，只要将代数数域的生成元一次映射成 γ，一次映射成 $-\gamma$ 即可. 如命

$$\eta = a + b\vartheta,$$

则所要求的两个賦値就是

(9) $$\varphi_{p1}(\eta) = \varphi_p(a + b\gamma),$$

(10) $$\varphi_{p2}(\eta) = \varphi_p(a - b\gamma).$$

由于 Ω_p 的 p-adic 賦値 φ_p 是已知的，故 φ_{p1} 和 φ_{p2} 也就随之完全确定.

还可以指出，在具体的情况下，并沒有必要将模 $p, p^2, \cdots$ 的

无限多个同余类全部計算出来，經过有限多步之后就可以中断这一过程。事实上，决定賦值 $\varphi_p(a+b\gamma)$ 时，起决定作用的是 p-adic 数 $a+b\gamma$ 能被 p 的怎样一个幂整除。举例来說，如果經过三步之后可以断定它能被 p^2 整除，而不能被 p^3 整除，則

$$\varphi_p(a+b\gamma)=p^{-2}.$$

余下来需要討論的，是判别式的两个素因子 $p=2$ 和 $p=5$。

根据 Eisenstein 准則，$F(x)=x^2-5$ 在 Ω_5 中是不可約的，因为在这个多項式中，除头一个系数之外，所有系数都能被 5 整除，而最末一个系数不能被 5^2 整除。因此 (7) 对 $p=5$ 也成立。

在 Ω_2 中 Eisenstein 准則不再适用。可是如果我們命 $x=2y+1$，則有

$$x^2-5=(2y+1)^2-5=4(y^2+y-1),$$

而 y^2+y-1 模 2 不可約。因此 x^2-5 是 2-adic 不可約的，(7) 对 $p=2$ 也成立。

习題． 1. 多項式 x^2+1 在实数域和域 Ω_2 中都不可約。以某一奇素数 p 为模这个多項式是否可約，視 $p=4k+1$ 或 $p=4k-1$ 而定。[同余类域 $GF(p)$ 的乘法羣是一个 $(p-1)$ 阶巡迴羣。它是否包含四次单位根，視 $(p-1)$ 能否被 4 除尽而定.]

2. 試确定 Gauβ 数 $a+bi$ 所成的域的全部賦值。一共有多少个阿基米德賦值？对怎样的 p 有两个賦值，对怎样的 p 只有一个賦值？

代数数域的 p-adic 賦值和代数整数环內的素理想有着非常密切的关系。在第二卷中我們还要回到这个問題上来。

§ 80. 有理函数域 $\Delta(x)$ 的賦值

任意一个域 Δ（"常数"域）都可以添加一个不定元 x 而得有理函数域 $\Delta(x)$。我們要找出有理函数域 $\Delta(x)$ 的那样一些賦值，在这些賦值中 Δ 中所有非零常数具有值 1。

特别，在这样的赋值中所有和 $1+1+\cdots+1$ 有值 1. 因此，这种赋值是非阿基米德赋值. 如果把它表成指数形式

$$\varphi = e^{-w},$$

则对所有常数 a 有 $w(a)=0$.

可能出现两种不同的情况：

1. 对所有多項式 $f(x)$, $w(f)\geqslant 0$;

2. 存在一个多項式 $f(x)$，使得 $w(f)<0$.

可能对所有多項式 f 都有 $w(f)=0$. 在这一情形下所有的商 f/g 也都有值 0，所考虑的赋值是不足道的.

除去这一情况外，在第一种情形下存在一个多項式 f，使得 $w(f)>0$. 如果将 f 分解成素因子，那末至少有一个素因子的值 >0.

設这个素因子是 $p(x)$，而其值为 $v=w(p)$，则每个不能被 $p(x)$ 整除的多项式的值都为零. 事实上，設 $q(x)$ 是一个不能被 $p(x)$ 整除的多項式，而其值 >0，那末由于 p 和 q 互素，故有

$$1 = Ap + Bq,$$

其中 A 和 B 都是多項式. 由此即可得

$$w(Ap) = w(A) + w(p) > 0,$$

$$w(Bq) = w(B) + w(q) > 0,$$

因而据非阿基米德赋值的基本性質有

$$w(1) = w(Ap + Bq) > 0,$$

而这是不可能的.

設 $f(x)$ 是一个任意的多項式，并命

$$f(x) = p(x)^m q(x),$$

其中 $q(x)$ 不再能被 $p(x)$ 整除，则 $f(x)$ 的值立即可以得出：

$$w(f) = mw(p) + w(q) = mv.$$

对于多项式的商象通常一样有

$$w\left(\frac{f}{g}\right) = w(f) - w(g).$$

因此，在第一种情形下所考虑的賦值等价于由一个素多项式 $p = p(x)$ 所定义的 p-adic 賦值. 这种賦值和有理数域的 p-adic 賦值完全相似.

特别簡单的情形是常数域Δ为一代数封閉域的情形. 这时除了一次式

$$p(x) = x - a$$

之外不再有其他的素多项式.

相应于 Δ 中的每个 a 恰有一个素多项式 $p = x - a$, 因而也恰有一个 p-adic 賦值. 当我們把 a 看作是一个复平面上的一个点时,这个賦值称为属于点 a 的賦值. 如果一个多项式恰被 $(x-a)^m$ 整除，或者說，这个多项式以 a 为它的一的 m 阶零点,那末在这个賦值下多项式的值是 m. 如果一个有理函数 $\varphi = f/g$ 的分子能被 $(x - a)^m$ 整除,而分母不能被 $x - a$ 整除,它的值也是 m. 如果情况恰恰与此相反，則 φ 以 a 为它的一个"m 阶极点"，而 φ 的值 $w(\varphi)$ 是 $-m$.

这样,第一种情形就完全解决了. 現在我們要証明,在第二种情況下,除等价賦值外只有唯一的一个賦值,卽

$$w\left(\frac{f}{g}\right) = -m + n,$$

其中 m 为分子 f 的次数,而 n 为分母 g 的次数.

証明. 設 $p(x)$ 是使得 $w(p) < 0$ 的一个次数最低的多项式. $p(x)$ 的次数不可能为零，因为根据我們的假設，所有常数都有值零. 另一方面，$p(x)$ 的次数也不可能大于 1. 事实上，如果

$$p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n, \quad n > 1, \quad a_0 \neq 0,$$

則多項式 x 的次数較 $p(x)$ 的次数为低，因而有值 $w(x) \geqslant 0$，从而多項式 a_0x^n 也具有一个 $\geqslant 0$ 的值。另一方面，多項式 $a_1x^{n-1} + \cdots + a_n$ 的次数也低于 $p(x)$ 的次数，故其値也是 $\geqslant 0$ 的。这样一来，和

$$p(x) = ax^n + (a_1x^{n-1} + \cdots + a_n)$$

的値也 $\geqslant 0$，而这是与所設相违的。

因此，$p(x)$ 是一次多項式：

$$p(x) = x - c.$$

現設

$$q(x) = x - b = (x - c) + (c - b)$$

为另一个一次多項式，則由于 $w(x - c) < w(c - b)$，故根据早些时候所作过的一个注記应有

$$w(q) = \min(w(x - c),\quad w(c - b)) = w(p).$$

这就是說，所有的一次多項式都具有同一負值 $w(p) = w(q) = -v$。

我們总可以由所考虑的賦值过渡到一个等价的賦值，使得 $v = 1$。这时所有一次多項式都有値 -1。

所有的冪 x^k 都具有值 $-k$，乘上一个常数因子之后也不会改变它們的值，因此

$$w(ax^k) = -k.$$

最后，每个多項式 f 都是一些形为 ax^k 的項的和。根据前面所作过的注記，f 的值 $w(f)$ 应等于各个項之值的最小者。如 f 的次数为 n，則

$$w(f) = -n,$$

这就証明了我們的定理。

这样，有理函数域 $\Delta(x)$ 在无限多个 p-adic 賦值之外，还有一

个按次数的赋值，恰好象有理数域除无限多个 p-adic 賦值之外还有一个絕对值賦值一样．可是这种类似并非完全的，因为按次数的賦值是非阿基米德賦值，而絕对值賦值卻是阿基米德賦值．

在有理数域的情形，一个阿基米德賦值和无限多个 p-adic 賦值之間存在着重大的差别．在有理函数域的情形，按次数的賦值和 p-adic 賦值却是属于同一性质的．説得更确切些：通过一个非常簡单的域同构可把按次数的賦值轉变为任意 p-adic 賦值．事实上(参看 § 63)，如命

$$x = \frac{1}{y - c}, \tag{1}$$

則次数为 m 和 n 的两个多項式的商

$$\varphi(x) = \frac{f(x)}{g(x)} = \frac{ax^m + \cdots}{bx^n + \cdots}$$

經过代换(1)，并将分子分母都乘以 $(y - c)^{m+n}$ 之后，就成为 y 的两个多項式的商，其分子可被 $(y - c)^n$ 整除，分母可被 $(y - c)^m$ 整除．在属于点 c 的賦值中，商 $\psi(y)$ 的值是 $n - m$．这样，同构(1)就把域 $\Delta(x)$ 的按次数的賦值轉变成为同构域 $\Delta(y)$ 的属于点 c 的賦值．

由(1)可以看出，和"点" $y = c$ 相对应的是"点" $x = \infty$．因此我們説，按次数的賦值是**函数域 $\Delta(x)$ 的属于点 ∞ 的賦值**．复平面添加一个点 ∞ 之后即成为球面，而在球面上所有的点都是同等的．分式綫性变换

$$y = \frac{ax + b}{cx + d} \tag{2}$$

将球面上的每个点变成每个另外的点．(1)显然是(2)的一个特例．

現在我們問：相应于域的不同的"位"，能够作出怎样一些完备

域来．早些时候（§ 75）我們已經看到，和 $p = x - c$ 相应的完备域，即所有形式冪級数

$$\alpha = a_{-m}(x-c)^{-m} + \cdots + a_0 + a_1(x-c) + a_2(x-c)^2 + \cdots$$

所成的域．冪級数的系数为完全任意的常数．不論系数如何选择，冪級数在 p-adic 賦值的意义下是收斂的．当 c 为复数时，冪級数在函数論的意义下不一定收斂：收斂半径完全可能等于零．

如果 a_{-m} 是上面所写出的冪級数中第一个不为零的系数，則这个冪級数的值 $w(\alpha)$ 等于 $-m$．

与此完全类似，和点 $x = \infty$ 相应的完备域即 x^{-1} 的所有冪級数

$$\beta = b_{-m}x^m + \cdots + b_0 + b_1x^{-1} + b_2x^{-2} + \cdots$$

所成的域．

§ 81. 代数函数域的賦值

一个变量 x 的代数函域，指的就是有理函数域 $\Delta(x)$ 的一个有限扩域．为簡单起见，我們假定这个扩域是单純的：

$$\Lambda = \Delta(x, \vartheta).$$

其次，我們假定 Δ 是代数封閉的．

我們要找出域 Λ 的所有那样的賦值，在这种賦值下 Δ 中的常数全都具有值 $\varphi(a) = 1$，因而具有指数 $w(a) = 0$．

为了这个目的，我們从域 $\Delta(x)$ 的一个具有同样性质的任意賦值出发．根据 § 80，这样一个賦值必属于某一点 $x = c$ 或 $x = \infty$．只要我們取 $x - c$ 或 x^{-1} 为新变量，总可以假定这个賦值是属于点 $x = 0$ 的．这时，相应的完备扩域 Ω 就是 x 的所有冪級数所成的域．指数 $w(\eta)$，或者象我們在下文中所說的那样，冪級数 $\eta = c_mx^m + \cdots$ 的阶，等于第一个不为零的项的指数：

$$w(\eta) = m.$$

为了将这一賦值开拓成 Λ 的一个賦值，必須将以 ϑ 为零点的規范化[1]不可約多項式 $F(z)$ 在域 Ω 中分解成素因子

(1) $$F(z) = F_1(z)F_2(z)\cdots F_s(z).$$

这样，因子 $F_\nu(z)$ 就是 z 的多項式，而其系数則为 x 的冪級数. 現在我們将每个这样的因子 $F_\nu(x)$ 的一个零点 ϑ_ν 添加到 Ω 上去，并按照 § 77 中的方法通过

$$W(\eta) = n_\nu^{-1}w(N(\eta))$$

来定义 $\Omega(\vartheta_\nu)$ 的賦值，其中 n_ν 为 F_ν 的次数，而范数則是在 $\Omega(\vartheta_\nu)$ 中作出的. 如果依次命 ϑ 为 $\vartheta_1, \vartheta_2, \cdots, \vartheta_s$，就可得出 Λ 的賦値 $W_1, W_2, \cdots, W_s$. 同构 $\vartheta \to \vartheta_\nu$ 将任意域元素

$$\eta = g(\vartheta)$$

变成

$$\eta_\nu = g(\vartheta_\nu),$$

即相应的賦值为

(2) $$W_\nu(\eta) = W(\eta_\nu) = n_\nu^{-1}w(N(\eta_\nu)).$$

一切都和代数数域的情形完全类似，只是更簡单一些，因为分解(1)可由代数函数的冪級数展开的古典方法得出. 級数展开的理論的最簡单的形式可在 Ostrowski[2]（对特征零）和 Ancochea[3]（对特征 p）的工作中找到. 为了得到和古典函数論的联系，我們先考虑复数域的情形，然后再看怎样把所得概念和定理拓广到一般情形.

因此，我們設 Δ 为复数域. 我們先假定，当 $x = 0$ 时規范化多項式 $F(z)$ 所有的系数都是有限的，并且判别式不等于零. 因此，

1) “規范化”仍是指首項系数为 1.

2) Ostrowski, A., *Math. Z.*, **37** (1933), 98—133.

3) Ancochea, G., *Acta Salamanticensia*, **1** (1946), 10.

在点 $x=0$ 的一个圆邻域 $|x|<R$ 内这个多项式恰有 n 个互异根 $\vartheta_1, \cdots, \vartheta_n$; 这 n 个根是 x 的正則函数，因而可展成 x 的冪級数[1]:

$$\vartheta_\nu = a_{\nu 0} + a_{\nu 1}x + a_{\nu 2}x^2 + \cdots. \tag{3}$$

在这个冪級数中，我們可按照自己的意愿把 x 看作未定元或看作一个复变量。如果我們象直到目前为止所作的那样，把 x 看作未定元，則冪級数 ϑ_ν 完全形式地满足方程 $F(\vartheta_\nu)=0$. 也就是說，当我們把它代到方程中去，并按 x 的冪展开，則各个項都等于零。另一方面，我們也可以把 x 看成一个复变数，也就是說，可以取圓 $|x|<R$ 內的任意复数来代替 x. 这时冪級数在普通的意义下收斂，并且作为复数来看满足方程 $F(\vartheta_\nu)=0$.

不論我們采取这两种看法中的哪一种，$F(z)$ 总是完全分解成一次因子

$$F(z)=(z-\vartheta_1)(z-\vartheta_2)\cdots(z-\vartheta_n). \tag{4}$$

因此，在 (2) 中所有 $n_\nu=1$，范数也不出現，属于点 $x=0$ 的 n 个賦值簡单地由

$$W_\nu(\eta)=w(\eta_\nu)$$

給出，其中 η_ν 就是由 $\eta=g(\vartheta)$ 經过变量代換 $\vartheta=\vartheta_\nu$ 所得到的冪級数。

上述情况也可以表述成如下的形式：在圓 $|x|<R$ 之上有代数函数 ϑ 的 Riemann 面的 n 个不分支的叶。在每个叶上函数 $\eta=g(\vartheta)$ 由冪級数 $\eta_\nu=g(\vartheta_\nu)$ 表示。如果这一冪級数以点 $x=0$ 为它的一个 m-阶零点（这里极点也看成零点，只不过它的阶数看成是負的），則

$$W_\nu(\eta)=w(\eta_\nu)=m.$$

---

1) 証明見函数論教科书或作者的"代数几何"(柏林, 1939), 53 頁.

当代数函数 ϑ 的 Riemann 面以 $x=0$ 为它的一个支点时，情况要稍許复杂些. 取圓 $|x|<R$ 足够小，使得在它里面沒有其它奇点，那末由上面的論証可知，在这个圓內的每个点 $x=c\neq 0$ 上有 Riemann 面的 n 个不同的叶. 这就是說，我們有 n 个解析函数 $\vartheta_1, \cdots, \vartheta_n$，它們在 $x=c$ 的近旁是正則的，并且滿足方程 $F(\vartheta_\nu)=0$.

当我們从点 $x=c$ 出发，沿着一个小圓周朝正方向繞行点 $x=0$ 一周时，函数 $\vartheta_1, \cdots, \vartheta_n$ 只能經受一个排列. 可設 $\vartheta_1, \vartheta_2, \cdots, \vartheta_k$ 受到一个循环排列，即繞行 $x=0$ 一周时，ϑ_1 連續地变成 ϑ_2 等等，而 ϑ_k 連續地变成 ϑ_1. 如果 $k>1$，我們就說，Riemann 面的 k 个叶在一个**支点**上彼此相接合.

$\vartheta_1, \cdots, \vartheta_k$ 的对称函数是在点 $x=0$ 的一个邻域中的单值解析函数. 除此之外，将这些对称函数乘上一个适当的冪 x^h 之后，可使得它們都是有界的，这可以很容易地由方程 $F(\vartheta_\nu)=0$ 看出. 因此，这些对称函数或者在圓 $|x|<R$ 內是正則的，或者以 $x=0$ 为其极点.

这样一来，积

$$F_1(z)=(z-\vartheta_1)\cdots(z-\vartheta_k) \tag{5}$$

就是 z 的一个多項式，其系数属于 x 的冪級数所成的域 Ω. 这个多項式的次数是 k.

多項式 $F_1(z)$ 在 $\Omega[z]$ 中是不可約的. 事实上，如果它是可分解的，那末在环繞点 0 时，它的根的一部分将会独自成为一組而彼此排列. 这样，我們就以函数論的方法作出了因子分解 (1) 中的一个不可約因子 (5). 由于每个这样的不可約因子只能决定一个賦值，故我們有下面的結果：

相应于代数函数 ϑ 的 Riemann 面上的每个点(不論其为支点

或否），恰有函数域 A 的一个赋值，并且通过这一方式可得出 A 的一切那样的赋值，在这种赋值下 Δ 中所有常数之值为 0.

在我們所討論的情形下，因子 $F_1(x)$ 的次数 n_1 等于 k.

在函数論里还可以証明，$\vartheta_1, \cdots, \vartheta_k$ 可表成"局部单値化变量"

$$t = x^{\frac{1}{k}}$$

的冪級数，并且只要在 ϑ_1 的冪級数中将 t 换成 $\zeta t, \cdots, \zeta^{k-1}t$ 就可以得出 $\vartheta_2, \cdots, \vartheta_k$ 的冪級数来，这里 ζ 是一个 k 次本原单位根：

$$\zeta = e^{\frac{2\pi i}{k}}.$$

将 ϑ 的这种冪級数表示依次代入 $\eta = g(\vartheta)$ 中去，就得到冪級数

$$\begin{aligned}
\eta_1 &= g(\vartheta_1) = c_m t^m + \cdots, \\
\eta_2 &= g(\vartheta_2) = c_m(\zeta t)^m + \cdots, \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\eta_k &= g(\vartheta_k) = c_m(\zeta^{k-1}t)^m + \cdots.
\end{aligned}$$

根据 (2)，为了找出指数赋值 W_1，首先必須作出范数 $N(\eta_1)$，即作出共軛元素的积 $\eta_1\eta_2\cdots\eta_k$. 这一乘积在代换 $t \to \zeta t$ 之下是不变的，因此它只含有 $t^k = x$ 的冪. 这样我們就得到

$$N(\eta_1) = \eta_1\eta_2\cdots\eta_k = Ct^{km} + \cdots = Cx^m + \cdots.$$

由 (2) 可知，所要求的赋值是

$$W_1(\eta) = k^{-1}m.$$

为了得出整数值，我們可以从这个赋値过渡到一个与之等价的赋值

$$W(\eta) = kW_1(\eta),$$

这时所得結果特别簡单，即有

$$W(\eta) = m.$$

用文字表达出来就是說：为了求得一个函数 $\eta = g(\vartheta)$ 的賦值，可将 $\vartheta_1, \cdots, \vartheta_k$ 按局部单值化变量展开的冪級数之一来代替其中的 ϑ，并决定出开头一項的指数.

§ 82. 抽象 Riemann 面

如果 Δ 不是复数域，那就不再有函数論或拓扑意义下的 Riemann 面. 但可以利用賦值的概念来作出 Riemann 面的一个純代数的代替品. 只要作如下的定义就行：

域 Λ 的一个位，就是使得所有常数之值为零的等价指数賦值 W 的一个类. 所有的位的全体称为抽象 Riemann 面.

由 (2) § 81 立即可以看出，所有这些賦值都是离散的：即存在一个最小的正値 $W(\pi) = W_0$. 过渡到一个等价的賦值，可以假定 $W_0 = 1$. 这时所有的 $W(\eta)$ 都是整数.

比較好的一种作法，就是避免把 $W(\eta)$ 称为"値"，以便在下文中在另一意义下使用这一名称. 因此，我們称 $W(\eta)$ 为函数 η 在位 S 上的阶. 如果阶是正的，且等于 m，那末我們就說这是一个 m-阶零点，如果阶是負的，且等于 $-h$，就說这是一个 h-阶极点（或 $-h$ 阶零点）.

一个具有最小正阶数 $W(\pi) = 1$ 的函数 π，称为位 S 上的局部单値化元素. 在一般情形下，局部单值化元素起着在复数域的情形下 k-次根 t 所起的作用. 我們馬上就会看到，域中所有的元素都可以展成 π 的冪級数. 对于代数理論来說，利用 π 較之利用 t 还有一个好处，即 π 是域 Λ 本身之內的一个元素.

象通常一样，相应于位 S 有一个賦值环 $\mathfrak{o}$，这个环由所有具有非負阶数的元素組成，还有一个賦値理想 $\mathfrak{p}$，由所有具有正阶数的元素組成.

$\mathfrak{p}$ 中所有的元素都是 π 的倍元. 事实上,設 η 具有正的阶数,那末这个阶数 $W(\eta)$ 最小应等于 1, 因此

$$W(\eta\pi^{-1}) = W(\eta) - W(\pi) \geqslant 1 - 1 = 0,$$

因而 $\eta\pi^{-1}$ 属于 $\mathfrak{o}$, 即 η 为 π 的倍元.

局部单值化元素 π 显然不会是一个常数,因此它对 Δ 来說不是代数的. 由于域 A 的超越次数为 1, 故 π 一个元素已經构成一个超越基,也就是說,域中的每个元素都是 π 的代数函数. 因此,对 $\mathfrak{o}$ 中的任意元素 η 有代数方程

$$g_0(\eta) + \pi g_1(\eta) + \cdots + \pi^h g_h(\eta) = 0.$$

如果 $g_0(\eta) = 0$, 則整个方程可以用 π 来除. 因此我們可以假定 $g_0(\eta) \neq 0$. 把这个方程变成一个模 $\mathfrak{p}$ 的同余式,就得到

$$g_0(\eta) \equiv 0(\mathfrak{p}). \tag{1}$$

因此,每个整元素 η 满足一个模 $\mathfrak{p}$ 的代数方程(1), 其系数为常数,且不全等于零. 这一事实也可以表述如下: $\mathfrak{o}/\mathfrak{p}$ 中的每个元素对 Δ 来說是代数的.

然而 Δ 是一代数封閉域, 故多項式 $g_0(\eta)$ 可以完全分解为一次因子,并且这些因子中必有一个是 $\equiv 0(\mathfrak{p})$ 的. 这就是說, η 同余于一个常数. 这就証明了:

$\mathfrak{o}$ 中的每个元素 η 模 $\mathfrak{p}$ 和一个常数 a_0 同余.

差 $\eta - a_0$ 是 $\mathfrak{p}$ 中的一个元素,因而是 π 的一个倍元:

$$\eta = a_0 + \eta_1\pi.$$

对 η_1 又可以重复同样的討論. 經过 n 步之后可得

$$\eta = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + \eta_n\pi^n.$$

无穷級数

$$a_0 + a_1\pi + a_2\pi^2 + \cdots$$

在賦值的意义之下收斂于极限 η. 事实上,由于

$$W(\eta_n\pi^n) \geqslant n,$$

故当 $n \to \infty$ 时，余項

$$\eta - (a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1}) = \eta_n\pi^n$$

有极限零。

这样，$\mathfrak{o}$ 中的每个元素 η 都可以展成 π 的冪級数

$$\eta = a_0 + a_1\pi + \cdots. \tag{2}$$

如果 η 不是整元素，那末我們可以将它乘上一个冪 π^h 使之成为整元素。将 $\eta\pi^h$ 展成 π 的冪級数再除以 π^h，就得 η 的一个冪級数

$$\eta = a_{-h}\pi^{-h} + \cdots + a_0 + a_1\pi + \cdots. \tag{3}$$

我們也可不說"位 S"而說"位 $\mathfrak{p}$"。事实上，位 S 由理想 $\mathfrak{p}$ 所唯一确定。

如果 $\eta \equiv a (\mathrm{mod}\ \mathfrak{p})$，我們就說：$\eta$ **在位** $\mathfrak{p}$ **上取值** a。如果 η 不是整元素，則 η 以位 $\mathfrak{p}$ 为它的一个极点；这时我們說：η **在位** $\mathfrak{p}$ **上取值** ∞。在这里，"值"这个名称具有不同于先前的意义：现在的所謂值不是实数 e^{-w}，它或者是常数域 Δ 中的一个元素，或者是符号 ∞。

这样定义的值 $\eta(\mathfrak{p})$ 具有下面的性質：

A. $(\eta + \zeta)(\mathfrak{p}) = \eta(\mathfrak{p}) + \zeta(\mathfrak{p})$，
B. $\eta\zeta(\mathfrak{p}) = \eta(\mathfrak{p}) \cdot \zeta(\mathfrak{p})$，
（A、B：如果 $\eta(\mathfrak{p})$ 和 $\zeta(\mathfrak{p})$ 均为有限。）

C. $\eta(\mathfrak{p}) = \infty$，如果 $\eta^{-1}(\mathfrak{p}) = 0$；反面也成立。

Dedekind 和 Weber 在他們的一个經典著作[1]中将"Riemann 面上一个点"的概念定义为一个具有性質 A. B. C. 的映射，并从这一定义出发导出了代数函数域的理論，关于这一理論的一个比

---

1) *J. reine u. angew. Math.*, **92** (1882).

較簡单和比較一般的論述，可以参看 F. K. Schmidt: *Math. Z.*, **41** (1936), 415—438.

关于賦値概念在代数几何上的应用，可以参看著者在 Jahresbericht der D. M. V. **52** (1942)161 頁中写的綜合評論，以及著者的論文 (*Math. Z.*, **51** (1948), 511 頁起的 § 4—8).

中 德 内 容 索 引

一至三画

四 画

五 画

六 画

七　画

八 画

九 画

十 画

十一画

十二画

十三画

十 四 画

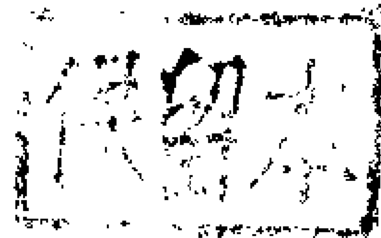
十 五 画

十六画

十七画

十八画

德中内容索引



統一书号：13031·1780

定　　价：　2.00 元

本社书号：2753·13-1